MAR 1 2 1982

1051-H-11

Y3.N88:25/2515/v.1

NUREG/CR-2515
SAND81-7229/I
AN
Printed December 1981

COMPLETED
193

CONTRACTOR REPORT

ORIGINAL

Crystal River-3 Safety Study
Volume I – Main Report

A. A. Garcia, Principal Investigator
R. T. Liner, P. J. Amico, E. V. Lofgren
Science Applications, Inc.
7315 Wisconsin Ave, Suite 1200 W
Bethesda, MD 20814

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

I

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from
GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

SAI-002-81-BE

NUREG/CR-2515/I of II
SAND81-7229/I of II

CRYSTAL RIVER-3 SAFETY STUDY

VOLUME I

MAIN REPORT

1 December 1981

Prepared by:

Science Applications, Inc.
7315 Wisconsin Avenue, Suite 1200W
Bethesda, Maryland 20814

Principal Investigator:

A. A. Garcia

Principal Authors:

R. T. Liner
P. J. Amico
E. V. Lofgren

Funded by
Division of Risk Analysis
Office of Nuclear Regulatory Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1241 (Sandia)
A6296 (EG&G)

Foreword

This report presents the results of an analysis of the Crystal River-3 (CR-3) plant performed as the Phase I project in the Interim Reliability Evaluation Program (IREP). The project had three original objectives: first, to perform a preliminary assessment of the level of risk associated with the CR-3 plant, and to compare this risk to that assessed for the two plants in the Reactor Safety Study; second, to provide support for the broader investigation by the Nuclear Regulatory Commission of the sensitivity of risk to feedwater perturbations associated with the once-through-steam-generator (OTSG) and the Integrated Control System (ICS) in plants equipped with reactors designed by the Babcock and Wilcox Company; and third, to provide a basis for the development of plans and procedures for IREP Phase II.

It was originally intended that the study be performed on the basis of "available data" and information on accident sequence phenomenology contained in the Reactor Safety Study. Several activities, however, went beyond the scope of the original study. These included a review of plant-specific failure rate data and incorporation of it into the analysis where appropriate; a review of reliability data for pumps, valves and diesels to obtain quantitative information on the probabilities of common mode failures; and a detailed analysis of important operator faults using the method known as Technique for Human Error Rate Prediction. In addition, the final results presented herein for CR-3 are based on results of directly applicable accident sequence phenomenology evaluations, published in May 1981, which were performed for a Babcock and Wilcox reactor by Battelle Columbus Laboratories in support of the Reactor Safety Study Methodology Applications Program (RSSMAP).

The CR-3 study employed several new techniques in risk assessment methodology which have been developed since the Reactor Safety Study. The most significant examples are the development of detailed transient event trees and the utilization of complement events in accident sequence description and evaluation. The study itself introduced "system interaction diagrams" as a tool for rapidly understanding and communicating the overall logical structure of plant systems and their dependencies on support systems.

The reader is cautioned to examine the results in context. The results provided here for individual accident sequences are not intended for direct comparison to the results of the Reactor Safety Study. Differences in reactor designs, advances in the state-of-the-art of risk assessment methodology and differences in the data used in the evaluations are but three of the reasons why such comparisons would be inappropriate.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the contributions of the many personnel involved at different times in the course of this project. At the beginning, G. J. Kolb of Sandia National Laboratories was instrumental in the development of the event trees for the plant. S. V. Asselin*, also of Sandia National Laboratories, performed special studies supporting the event tree development. A. F. McBride and J. W. Minarick of Science Applications, Inc., provided valuable assistance as consultants for systems interactions.

Also at the beginning, construction of the detailed and simplified system fault trees involved the following personnel:

M. E. Stewart J. E. Trainer	EG&G Idaho, Inc.
R. C. Bertucio J. Young	Energy, Inc.
M. A. Fedele	Evaluation Associates, Inc.
G. J. Kolb	Sandia National Laboratories
B. F. Putney	Science Applications, Inc.

During preparation of the preliminary draft report, H. F. Filacchione** of Science Applications, Inc., performed a major service in assembling, reviewing and editing many of the appendices to the report.

During preparation of this revised report, Duane W. Small of SAI Comsystems shared his human factors expertise in the evaluation of operator faults.

The authors acknowledge their responsibility for the final content of this report and for errors and omissions.

---

*Now with Technology for Energy Corporation

**Now with NUS Corporation

TABLE OF CONTENTS

Page

VOLUME I - MAIN REPORT

Foreword . . . . I-i

Acknowledgements . . . . I-ii

Table of Contents . . . . I-iii

List of Figures . . . . I-vi

List of Tables . . . . I-viii

Glossary . . . . I-x

1.0 INTRODUCTION 1-1

2.0 SUMMARY OF RESULTS 2-1

2.1 Frequency of Radioactivity Releases 2-1
2.2 Dominant Sequences 2-3
2.3 Functional and System Dependencies 2-16
2.4 Limitations of the Analysis 2-21

3.0 GENERAL PLANT DESCRIPTION 3-1

3.1 Reactor Coolant System (RCS) 3-6
3.2 Reactor Protection System (RPS) 3-6
3.3 Engineered Safeguards Actuation System (ESAS) 3-7
3.4 Engineered Safeguards Systems 3-7
3.4.1 Emergency Core Cooling System (ECCS) 3-8
3.4.2 Reactor Building Cooling and Spray Systems 3-11
3.5 Emergency Feedwater System (EFS) 3-12
3.6 Emergency Auxiliary Systems 3-12
3.6.1 Electric Power 3-13
3.6.2 Emergency Cooling Systems 3-13
3.7 Connections Between CR-3 and Coal-Fired Units 1 and 2 . . 3-15

TABLE OF CONTENTS

Page

4.0 EVENT TREES 4-1

4.1 Initiating Events 4-1
4.1.1 Transient Initiators 4-2
4.1.2 LOCA Initiators 4-3
4.2 Transient Event Tree 4-4
4.3 LOCA Event Tree 4-13
4.4 Special Events 4-19
4.4.1 Interfacing Systems LOCA (Event V) 4-19
4.4.2 Vessel Rupture 4-21
4.4.3 Steam Generator Tube Rupture 4-24
4.5 Containment Failure Modes 4-24
4.6 Radioactive Release Categories 4-27

5.0 FAULT AND EVENT TREE QUANTIFICATION PROCEDURES 5-1

5.1 Analytical Methods for Estimating Primary Event Probabilities 5-1
5.1.1 Fault Tree Development 5-1
5.1.2 Quantification Data Base 5-4
5.1.3 Evaluation of Hardware Faults 5-11
5.1.4 Evaluation of Human Faults 5-11
5.1.5 Evaluation of Common-Cause Faults 5-12
5.1.6 Evaluation of Test and Maintenance Outages 5-13
5.1.7 Evaluation of Interfacing System Faults 5-14
5.1.8 Evaluation of System Unreliability During Recirculation 5-15
5.2 Fault Tree Organization and Structure 5-17
5.2.1 A Fault Tree Hierarchy 5-18
5.2.2 System and Subsystem-Level Faults 5-20
5.2.3 Functional Level Faults 5-27
5.2.4 Fault Tree Quantification Tables 5-29

TABLE OF CONTENTS

Page

5.3 Sequence Analysis 5-34
  5.3.1 Boolean Reduction of Event Tree Sequences 5-34
  5.3.2 Initiating Event Frequencies 5-37
  5.3.3 Probabilities for Special Events in the Transient Event Tree 5-38
  5.3.4 Analysis of ATWS Sequence 5-40
  5.3.5 Containment Failure Probabilities 5-46
  5.3.6 Accident Sequence Analysis Results 5-48
5.4 Analysis of Selected Operator Faults 5-66

VOLUME II - APPENDICES

Table of Contents . . . . II-i

Glossary . . . . II-iv

Introduction II-1

Appendix A - Reactor Protection System (RPS) A-1
Appendix B - Engineered Safeguards Actuation System (ESAS) B-1
Appendix C - DC Power System C-1
Appendix D - Class I.E. AC Power System D-1
Appendix E - Nuclear Services Closed Cycle Cooling System (NSCCCS) E-1
Appendix F - Decay Heat Closed Cycle Cooling System (DHCCCS) . . . F-1
Appendix G - High Pressure Injection and Recirculation System . . G-1
Appendix H - Core Flood System (CFS) H-1
Appendix K - Low Pressure Injection and Recirculation System . . K-1
Appendix L - Reactor Building Emergency Cooling System (RBECS) . . L-1
Appendix M - Reactor Building Spray System (RBSS) M-1
Appendix N - Reactor Building Isolation System (RBIS) N-1
Appendix P - Emergency Feedwater System (EFS) P-1

LIST OF FIGURES

Page

1.1 Schematic Approach to Probabilistic Risk Assessment for Crystal River-3 Safety Study 1-5

2.1 Comparison of Crystal River-3 and Surry-1 Release Frequencies in Reactor Safety Study Radioactivity Release Categories for PWR 2-2

2.2 Dependencies on Emergency Cooling Systems in Crystal River-3 . . 2-14

2.3 Dependencies on Emergency Electric Power and Cooling Systems in Crystal River-3 2-15

2.4 System Interactions and Dominant Contributors to One of the Crystal River-3 Dominant Sequences (T_{2A} T_{10}) 2-17

3.1 CR-3 Site Layout Plan 3-2

3.2a Cross Section-Reactor Building and Auxiliary Building 3-3

3.2b Longitudinal Section-Reactor Building and Spent Fuel Building . . 3-4

3.3 Reactor Coolant System Arrangement Plan 3-5

3.4 Simplified Schematic Diagram of Engineered Safeguards System for Core and Building Protection 3-9

3.5 Simplified Schematic Diagram of the Emergency Cooling (NSCCS, DHCCCS) Systems 3-14

4.1 Minimal Emergency Coolant Injection Equipment Success Combinations for LOCA Events at CR-3 4-5

4.2 Transient Event Tree for Crystal River-3 4-7

4.3 LOCA Event Tree for Crystal River-3 4-14

4.4 Interfaces Between Reactor Coolant System and Low Pressure Systems 4-20

4.5 Fault Tree for Event V 4-22

4.6 PWR Containment Event Tree 4-25

5.1 Generic Modularized Fault Tree for "Safety System Fails or Unavailable" 5-3

5.2 Generic Modularized Fault Tree for "Safety System Fails During Recirculation" 5-16

5.3 Quantification Illustrations for ATWS Core Melt Sequences 25-30 for all Transient Initiators 5-43

LIST OF FIGURES (CONT.)

Page

5.4 Quantification Illustration for ATWS Core Melt Sequence 16 for all Type T_1 Transient Initiators 5-45

5.5 Quantification Illustration for ATWS Core Melt Sequence 21 for all Transient Initiators 5-47

5.6 Probability Estimation for Operator Fault H*02 5-71

5.7 Probability Estimation for Operator Fault L06 5-72

5.8 Probability Estimation for Operator Fault L017 5-73

5.9 Probability Estimation for Operator Fault L04 5-74

5.10 Probability Estimation for Operator Fault H01 5-75

5.11 Probability Estimation for Operator Fault H03 5-76

LIST OF TABLES

Page

4.1 Transient Event Frequencies 4-3

4.2 LOCA Frequencies 4-6

4.3 Event Definitions for Transient Event Tree 4-10

4.4 Definition of Equipment Success Requirements for Transient Events in Crystal River-3 4-12

4.5 Event Definition for LOCA Event Tree 4-16

4.6 Definition of ECCS Equipment Success Requirements for LOCA Events in Crystal River-3 4-18

4.7 Fault Summary Sheet for Event V Fault Tree for Crystal River-3 4-23

4.8 Containment Failure Modes and Probabilities 4-24

4.9 PWR Category Descriptions 4-29

4.10 Summary of Release Categories Representing Hypothetical Accidents 4-30

5.1a Mechanical Component Failure Rate Data 5-5

5.1b Electrical Component Failure Rate Data 5-6

5.2 Operating Availability History Data for Crystal River Units 1 and 2 5-7

5.3 Identification of System and Subsystem-Level Events Contributing to LOCA Event Tree Functions 5-21

5.4 Definitions of System and Subsystem-Level Boolean Variables Used in LOCA Sequence Analysis 5-22

5.5 Identification of System and Subsystem-Level Events Contributing to Transient Event Tree Functions 5-24

5.6 Definitions of System and Subsystem-Level Boolean Variables Used in Transient Sequence Analysis 5-25

5.7 Boolean Expressions for ECI and ECR 5-27

5.8 Boolean Equations for High Pressure Injection 5-30

5.9 Segment of Quantification Table for Events HA, HB and HPI 5-32

5.10 Containment Failure Mode Probabilities 5-46

5.11 Correspondence Among CR-3, Oconee, and Surry LOCA Sequences by Containment Failure Mode and Release Category 5-52

LIST OF TABLES (CONT.)

Page

5.12 Correspondence Among CR-3, Oconee, and Surry Transient Sequences by Containment Failure Modes and Release Category 5-53

5.13 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_1-T_{1A} Transient Initiators 5-54

5.14 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_{1A} Transient Initiators 5-55

5.15 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_2-T_{2A} Transient Initiators 5-56

5.16 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_{2A} Transient Initiators 5-57

5.17 Probabilities for B_1 Accident Sequences 5-58

5.18 Probabilities for B_2 Accident Sequences 5-59

5.19 Probabilities for B_3 Accident Sequences 5-60

5.20 Probabilities for B_4 Accident Sequences 5-61

5.21 Non-LOCA Transient Sequence Probabilities 5-62

5.22 Dominant Accident Sequences vs Release Categories for Transient Initiated Events 5-63

5.23 Dominant Accident Sequences vs Release Categories for LOCA Initiated Events 5-64

5.24 Dominant Accident Sequences vs Release Categories Tabulated in Decreasing Order-of-Magnitude of Sequence Probabilities . . . 5-65

GLOSSARY OF ABBREVIATIONS

A/E	Architect Engineer
ATWS	Anticipated Transient Without Scram
BWST	Borated Water Storage Tank
CRA	Control Rod Assembly
CFT	Core Flood Tanks
CR-3	Crystal River Unit 3
CRDM	Control Rod Drive Mechanism
DHCCCS	Decay Heat Closed Cycle Cooling System
DHCWS	Decay Heat Services Cooling Water System
DHSWS	Decay Heat Sea Water System
ECCS	Emergency Core Cooling System
ECF	Emergency Cooling Functionability
ECI	Emergency Coolant Injection
ECR	Emergency Coolant Recirculation
EFS	Emergency Feedwater System
EPRI	Electric Power Research Institute
ESAS (ESFAS)	Engineered Safeguards Actuation System
FSAR	Final Safety Analysis Report
HE	Heat Exchanger
HP, HPI, HPR	High Pressure (Injection) (Recirculation)
ICS	Integrated Control System
LOCA	Loss of Coolant Accident
LOSP	Loss of Offsite Power
LP, LPI, LPR	Low Pressure (Injection) (Recirculation)

GLOSSARY OF ABBREVIATIONS (CONT.)

MFW	Main Feedwater
MOV	Motor Operated Valve
NC, N.C.	Normally Closed
NO, N.O.	Normally Open
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NSCWS	Nuclear Service Cooling Water System
NSCCCS	Nuclear Services Closed Cycle Cooling System
NSSS	Nuclear Steam Supply System
NSSWS	Nuclear Services Sea Water System
OTSG	Once Through Steam Generator
PAHR	Post Accident Heat Removal
PARR	Post Accident Radioactivity Removal
PCS	Power Conversion System
PORV	Power Operated Relief Valve
RB(E)CS	Reactor Building (Emergency) Cooling System
RBIC	Reactor Building Isolation and Cooling
RBIS	Reactor Building Isolation System
RBSS, RBSI, RBSR	Reactor Building Spray System (Injection) (Recirculation)
RCS	Reactor Coolant System
RPS	Reactor Protection System
RSS	Reactor Safety Study (WASH-1400)
RSSMAP	Reactor Safety Study Methodology Applications Program
S/RV	Safety/Relief Valve

1.0 INTRODUCTION

This report provides a quantitative assessment of certain aspects of the public risk associated with operation of the Crystal River-3 (CR-3) nuclear power plant. The plant uses an 855 MWe pressurized water reactor whose nuclear steam supply system was manufactured by the Babcock and Wilcox (B&W) Company. The plant is located on the Gulf of Mexico at Crystal River, Florida, about 70 miles north of Tampa. It is operated and predominantly owned by the Florida Power Corporation.

The assessment includes estimates of the frequency (or probability per year) of radioactivity releases, in each of seven discrete categories, stemming from loss of coolant accidents (LOCAs) and various anticipated transients. The primary objective is to identify and estimate the probabilities of those types of accidents which are most likely to cause releases in these seven categories, and to identify and quantify the combinations of hardware and human faults which contribute most to these probabilities.

The most important contributors to the risk of radioactivity releases at CR-3, along with general conclusions and observations, are outlined in the next chapter. Suffice it to note here that the greatest risks at CR-3 appear to be associated with two distinct types of accidents. The first involves loss-of-offsite power transients and subsequent failures in the emergency electric power systems, sometimes combined with other hardware faults. Such accidents lead to releases in category 2 (the second most severe category) with an estimated frequency of about 3E-5 per year and in category 4 with a frequency about five times lower. These estimates are based on the national average frequency of loss of offsite power incidents (0.32 per year per plant); there is not sufficient data to establish the site-specific frequency of these incidents at CR-3 with reasonable confidence.

The most likely accidents involving core melt at CR-3 seem to be small-small LOCAs (effective area less than 0.087 sq. ft.) with failure of the high pressure cooling system in the recirculation mode and subsequent overpressure containment failure (in category 3) or melt-through of the containment building floor (in category 7). The estimated frequency of this accident sequence is relatively high, about 9E-5 per year in each of these categories. The high frequency results from the moderate frequency of the initiating event (~1.3E-3 per year) combined with the high likelihood of operator errors in the transition from coolant injection to coolant recirculation. The same basic sequence with containment failure by leakage is the dominant contributor in category 5, with an estimated frequency of about 1E-6 per year.

These and a few other sequences exhibit high estimated frequencies relative to many hundreds of other sequences analyzed at CR-3. They also lead to higher estimates of release frequencies in some categories, most notably the second and third, relative to the analogous estimates for Surry in the Reactor Safety Study (1-1). It would be highly premature, however, to make judgments of one reactor relative to the other because some of the differences in estimated sequence frequencies are undoubtedly due to variations in methods and assumptions. For example, many LOCA sequences at CR-3 are quantitatively dominated by operator faults that were not considered for Surry. Operator errors were considered rather explicitly for CR-3 and are important in essentially all the LOCA sequences. Moreover, operator error probabilities are among the most uncertain of all reliability parameters. A second example of analytical differences with the Reactor Safety Study concerns the loss of offsite power, where different assumptions were made regarding recoverability.

This study was performed in support of a broader investigation of the CR-3 plant whose objectives included, in addition to that stated above, assessment of the sensitivity of risk to feedwater perturbations associated with the once-through steam generator (OTSG) and the Integrated Control System (ICS), features which are unique to B&W nuclear plants. Participants in both aspects of the larger CR-3 analysis included the Nuclear Regulatory Commission Office of Regulatory Research, Sandia National Laboratory, the Idaho National Engineering Laboratory, and several private contractors.

The CR-3 project itself was initiated as Phase I of the Interim Reliability Evaluation Program (IREP), a more comprehensive risk assessment program intended to encompass all the commercial nuclear power plants in the United States (1-2).[1] Planning for these subsequent studies was begun during Phase I.

IREP was planned in recognition of the possibility that some nuclear plants might pose major risks from accident types that would not likely be apparent on the basis of perceptions and insight gained from the Reactor Safety Study. The objective of the program was to identify such "outliers" and assess their significance. CR-3 was chosen for the prototype study because it is representative of B&W plants. The B&W nuclear steam supply system is of particular interest in the wake of the incident at TMI-2 (1-3) and because of the sensitivity of the plant response to perturbations in the secondary system, especially the likelihood of overcooling transients. Some consideration was given also to the likelhood of loss-of-offsite-power incidents on the Florida peninsula.

The scope of the CR-3 safety analysis is limited on the one hand by the initiating events considered and, on the other hand, by the use of probabilities of radioactivity releases in discrete categories as a surrogate measure of risk. No consideration was given to the public consequences of accidents or to the meteorological or demographic characteristics of the site. The initiating events receiving the greatest attention by far include four size-categories of LOCAs and two major categories of transients (with and without normal secondary heat removal). Three other initiating events are discussed briefly and shown to pose negligible risks; these include failures at the interface of low and high pressure cooling systems, steam generator tube rupture, and reactor vessel rupture. The potential role of the Integrated Control System in an overcooling transient was addressed briefly, but it was found that meaningful results would require much greater depth and breadth of analysis than permitted by the scope of the study.

---

[1] The objectives and scope of IREP have since changed, as discussed briefly in the Foreword.

Hence, this problem as well as the more general problem of operational sensitivity of the secondary cooling system are not addressed in this report.

A further limitation of the present study is that all calculations of probabilities are in terms of "point estimates." The calculations rely entirely on point estimates of component and human reliability parameters. Uncertainties are investigated neither by error propagation nor by sensitivity studies. This limitation lowers the confidence that one could place in the results as basis for major design-related decisions, but it does not preclude use of the results in the preliminary identification and characterization of outlying contributors to risk. It is noted that much of the information which would be necessary for uncertainty studies is included in the appendices, and that the NRC is presently considering such an uncertainty study for future work.

The analytical approach follows in basic outline the event tree/fault tree analysis first pioneered by the Reactor Safety Study. There are differences in some details and the scope is limited with respect to accident consequences and uncertainty analysis as indicated above; moreover, the present study draws directly upon the Reactor Safety Study for certain aspects of the analysis, most notably the definition of radioactivity release categories. It also draws on the RSSMAP Oconee report (1-4) for more recent and directly applicable information related to analysis of containment failure modes and probabilities. The present adaptation of the general approach is simply illustrated in Figure 1.1.

The analysis resulted in the construction of two generic event trees, one for transients and one for LOCAs. These were adapted to their respective subcategories and also were combined to represent transient-induced LOCAs. "Top Events" were defined as required by the event trees for all the major systems and the corresponding fault trees were constructed and evaluated. In many cases, systems were involved in several top events and therefore required several closely related but different fault trees.

Upon completion of the initial estimation of sequence probabilities and the correlation of sequences with release categories, those sequences making dominant contributions to the likelihood of a release in any given category were identified. Operator faults contributing significantly to any of these sequences were subjected to detailed analysis on the basis of human factor principles. The probabilities of the corresponding sequences were subsequently refined on the basis of this analysis.

Two aspects of the analysis are more advanced than their Reactor Safety Study counterparts. First, for each system, the complete spectrum of top events arising from the event trees for the various accident initiators is defined explicitly. The initial system fault trees were adapted for each event and evaluated accordingly. In the Reactor Safety Study, in most cases a single top event was used to represent a system wherever it appeared in the event trees. Second, in this study system interdependencies were rigorously treated by means of Boolean reduction (the code WAMCUT (1-5) was used to facilitate this part of the analysis). In the Reactor Safety Study, adjustments were made to the quantitative results to account for system interdependencies.

The next chapter provides a summary of the release probabilities; it identifies and describes the sequences which make the dominant contributions to the probability of releases in the seven categories employed. It also identifies the combinations of faults most likely to cause each sequence. Some general observations on system interdependencies and a more complete discussion of major assumptions and limitations of the study are presented. Chapter 3 provides a brief description of the CR-3 plant. Chapter 4 presents the event trees and discusses their construction.

Quantification of both the fault trees and the event trees is the subject of Chapter 5. An overview of the basic analytical methods is presented first, followed by a discussion of the fault tree analysis, including a guide to the detailed fault tree analyses which appear in the separately bound appendices. Finally, event tree quantification is discussed and the most important results are presented. Various intermediate sequence probabilities are also presented for the benefit of those readers specifically interested in details of the quantification process.

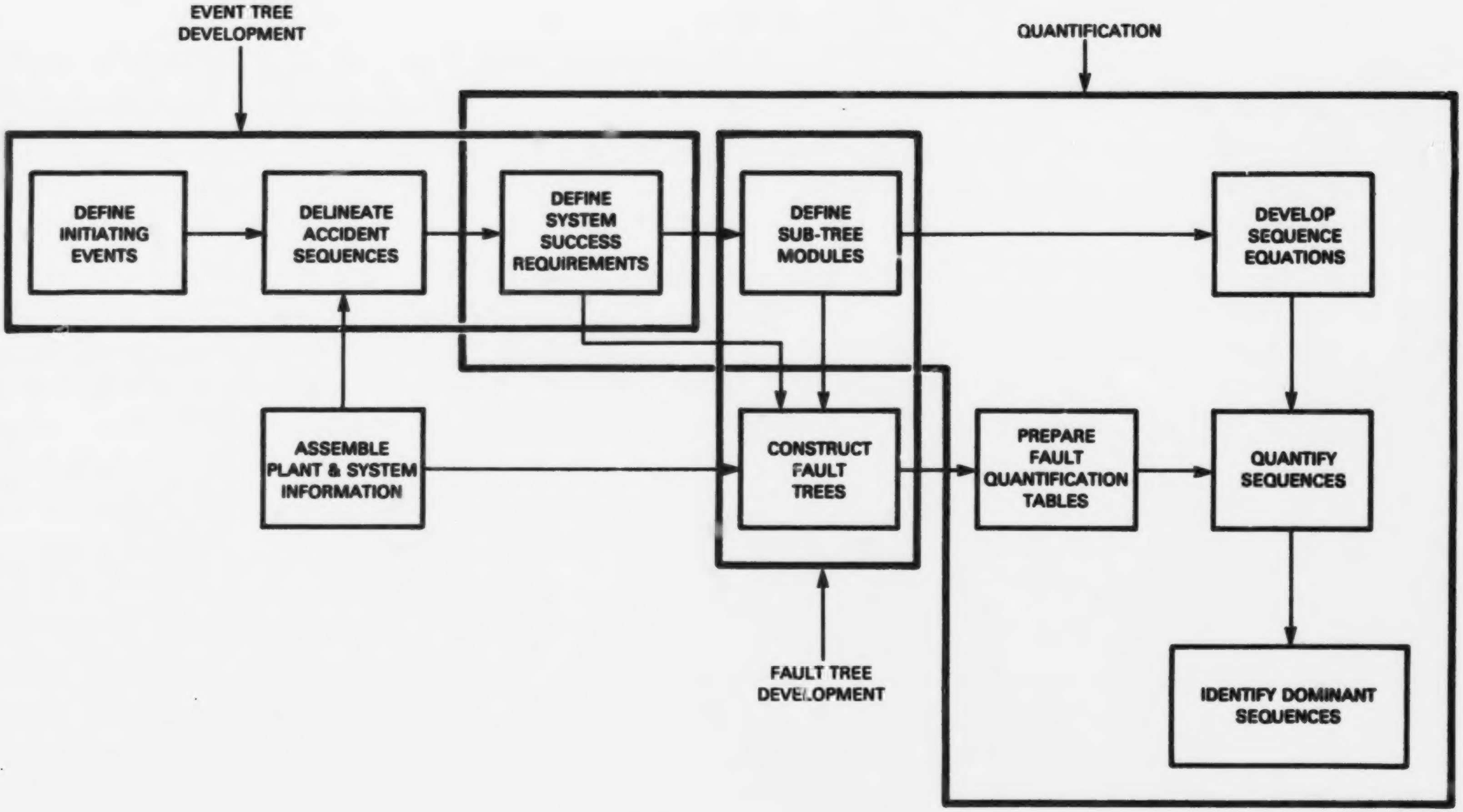

EVENT TREE DEVELOPMENT
QUANTIFICATION
DEFINE INITIATING EVENTS
DELINEATE ACCIDENT SEQUENCES
DEFINE SYSTEM SUCCESS REQUIREMENTS
DEFINE SUB-TREE MODULES
DEVELOP SEQUENCE EQUATIONS
ASSEMBLE PLANT & SYSTEM INFORMATION
CONSTRUCT FAULT TREES
PREPARE FAULT QUANTIFICATION TABLES
QUANTIFY SEQUENCES
FAULT TREE DEVELOPMENT
IDENTIFY DOMINANT SEQUENCES

FIGURE 1.1. SCHEMATIC APPROACH TO PROBABILISTIC RISK ASSESSMENT FOR CRYSTAL RIVER-3 SAFETY STUDY

References

1-1 U.S. Nuclear Regulatory Commission, "Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

1-2 U.S. Nuclear Regulatory Commission, "Integrated Reliability Evaluation Program, RES/PAS FY 1980 Program Brief," Attachment to Standard Order for DOE Work SOEW 60-80-031, November 16, 1979.

1-3 The President's Commission on the Accident at Three Mile Island, "The Accident at Three Mile Island," October 1979.

1-4 C.J. Kolb, S.W. Hatch, P. Cybulskis and R.O. Wooton, Sandia National Laboratories, "Reactor Safety Study Methodology Applications Program: Oconee No 3 PWR Power Plant," USNRC Report NUREG/CR-1659 (2 of 4) January 1981, Revised May 1981.

1-5 R.C. Erdmann, F.L. Leverenz, H. Kirch and G.S. Lellouche, Electric Power Research Institute," WAMCUT, A Computer Code for Fault Tree Evaluation," EPRI NP-803, 1978.

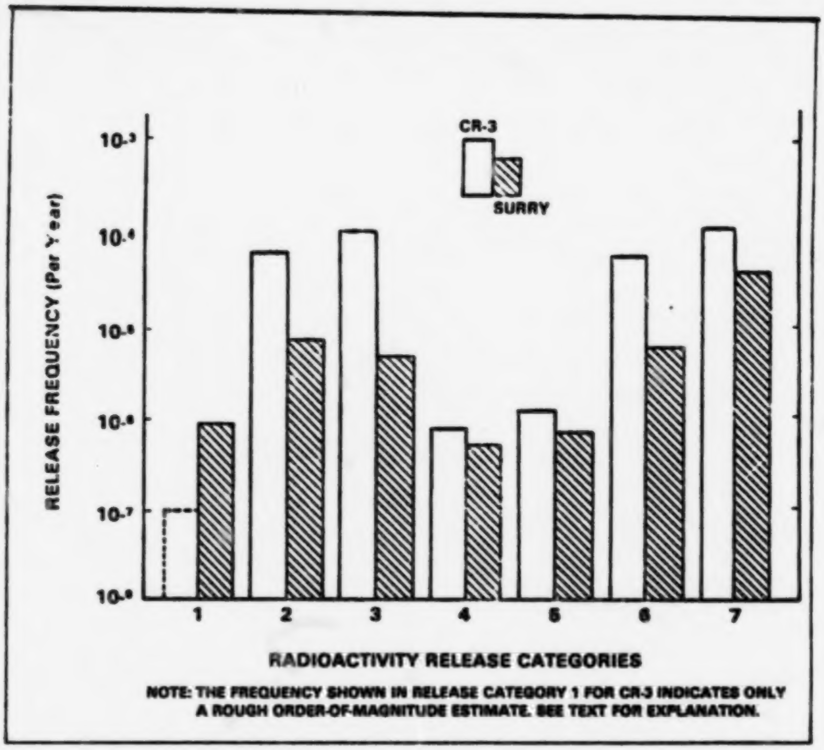
2.0 SUMMARY OF RESULTS

The basic results of the CR-3 study are the estimated frequencies of accident sequences identified with each of seven different radioactivity release categories. To place these results in perspective, we first present the total estimated frequency in each category and compare this composite result with the same result from the Reactor Safety Study Analysis of Surry (2-1). Next, we identify and describe the important CR-3 sequences which dominate the release frequency in each category. In Section 2.3, we discuss the important functional dependencies and system interactions at CR-3 and suggest some considerations for possibly improving the safety of the plant. Finally, in Section 2.4 we outline the major assumptions and limitations of the study so as to shed some light on the general applicability of the results and observations.

2.1 Frequency of Radioactivity Releases

The estimated frequencies of releases in each category at CR-3 are shown graphically in Figure 2.1, where they are compared to the same basic information for Surry. The release categories are numbered in order of decreasing severity; with other factors equal, the trend in risk would be the same. However, a quantitative relationship among the degrees of risk associated with different categories is neither implied nor intended. The frequencies for Surry have been subjected to a "smoothing" technique wherein 10% of the frequency in each category is assigned to adjacent categories; categories 1, 4 and 5 are dominated by this "10% contribution." This means the frequencies in these categories are not directly related to specific accident sequences. No smoothing technique has been applied to the CR-3 results. The frequency for category 1 at CR-3 is shown by a dashed line to indicate only a rough order-of-magnitude for this category because all accident sequences assigned to this release category had calculated values $\leq$ 1E-7/year, the cutoff value used in the sequence evaluation.

Initial appearances perhaps to the contrary, the differences in risk posed by the two reactors are probably not as great as the uncertainty in



NOTE: THE FREQUENCY SHOWN IN RELEASE CATEGORY 1 FOR CR-3 INDICATES ONLY A ROUGH ORDER-OF-MAGNITUDE ESTIMATE. SEE TEXT FOR EXPLANATION.

Figure 2.1 Comparison of Crystal River-3 and Surry-1 Release Frequencies in Reactor Safety Study Radioactivity Release Categories for PWR

our quantitative estimates of sequence frequencies. The most significant apparent differences between Surry and CR-3 are clearly in categories 1 and 3, followed closely by the differences in categories 2 and 6. In all of these categories except category 1, CR-3 appears to have the highest release probabilities, particularly so in category 3.

Categories 3, 5 and 7 at CR-3 are dominated quantitatively by small-small LOCA sequences in which operator errors are the most likely causes of system failures. Some of the operator errors in these and other sequences are major contributors to sequence frequencies, yet they are of a type that were not included in the earlier analysis of Surry. This suggests two things: one, apparent differences between Surry and CR-3 are as likely to be methodological as real; two, the model used to represent operator faults may be as responsible for uncertainty as the uncertainties in the human error probabilities assigned to elements in the model.

Other methodological issues that could account for some differences between the Surry and CR-3 analyses include the method of treating common mode faults, the use of more sophisticated sequence evaluation techniques in the CR-3 analysis, and differences in failure rate data.

One of the dominant sequences in category 2 at CR-3 is initiated by loss-of-offsite power. This highlights the fact that risk is sensitive not only to the frequency of offsite power losses but also to the likelihood of recovering offsite power in a short time. Potential differences between plants may be obscured by the use of "national average" data when the appropriate frequencies may well be highly site-dependent.

With obvious differences in analytical methods and with identified sensitivities to highly uncertain parameters, it would be premature to make judgments regarding the relative merits of different reactors. The analysis here best serves to identify apparent differences between plants for further investigation and to focus attention on the most vulnerable characteristics of a particular plant, in this case CR-3.

2.2 Dominant Sequences

Eight basic sequences, exclusive of variations in the mechanisms of containment failure and of the size-range of LOCA break sizes, have been identified as the most important contributors to public risk at CR-3. These sequences essentially consist of all those identified in release category 2 with frequency greater than 1E-7/year, those in release category 3 with frequency greater than 4E-6/year, and those in the remaining release categories with frequency greater than 1E-5/year. (No sequences were identified in release category 1 with frequency greater than 1E-7/year.) All of these dominant sequences are briefly described below. A symbolic representation of each sequence, the basis of which is described in a later chapter, is indicated for subsequent reference; the estimated frequency is also provided. Within each description, the particular combinations of hardware and human faults which contribute most to the sequence frequency are delineated.

a. Small-Small LOCA Followed by Failure of Emergency Coolant Injection and Reactor Building Spray Injection (Sequence B_4S_{23}; 6.5E-5/yr)

This sequence is initiated by a small-small LOCA followed by failure of emergency coolant injection (ECI) and reactor building spray injection (RBSI). In this sequence, the initial loss of coolant through the break is not replenished due to the loss of ECI at some time during the injection phase of the accident. This results in the eventual uncovering of the core and subsequent core melt. In addition, the sprays are not available to remove radioactivity from the containment atmosphere, although containment overpressure is still controlled by the reactor building fans.

This sequence dominates release categories 2, 4 and 6. It contributes about 50% to category 2 when containment failure results from hydrogen burning, about 55% to category 4 when containment failure results from leakage, and about 45% to category 6 when containment failure results from melt-through.

As indicated below, by far the most likely cause of this sequence (given the initiating event) is an operator fault in which the valve realignment from injection to recirculation is made prematurely.

Failure Mode (Cut Set): B4•L017 (6.5E-5/yr; ~100%)

B_4 = Initiating Event: Small-small LOCA (1.3E-3/yr)

L017 = Operator switches to recirculation prematurely; pump failure results from insufficient water in the sump. (0.05/demand)

With insufficient water in the reactor building sump, both the ECI and the RBSI pumps lose suction due to lack of cooling.

The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ), and 0.007 for containment leakage (β).

This sequence can also be initiated by larger LOCAs, whose smaller frequencies result in correspondingly smaller frequencies for the new sequences, as follows: B_3S_{23}, 5.1E-6/yr; B_2S_{23}, 5.0E-6/yr; and B_1S_{23}, 5.0E-6/yr. These sequences, as a group, contribute about 5% to category 2 when containment failure results from hydrogen burning and about 15% to category 6 when containment failure results from melt-through.

The dominant failure modes and cut sets for these sequences are the same as for B_4S_{23}, differing only in the initiating event probabilities.

Failure Mode (Cut Set): $B_3 \bullet$L017 (5.1E-6/yr; ~98%)
B_3 = Initiating Event: Small LOCA (1.0E-3/yr)
L017 Defined above (0.05/demand)

Failure Mode (Cut Set): $B_2 \bullet$L017 (5.0E-6/yr; ~100%)
B_2 = Initiating Event: Medium LOCA (1.0E-4/yr)
L017 Defined above (0.05/demand)

Failure Mode (Cut Set): $B_1 \bullet$L017 (5.0E-6/yr; ~100%)
B_1 = Initiating Event: Large LOCA (1.0E-4/yr)
L017 Defined above (0.05/demand)

The containment failure modes and release categories for all three of these sequences are the same as for B_4S_{23}. The containment failure mode probabilities for each of the sequences initiated by these larger LOCAs are 0.2 for hydrogen burning (γ) and 0.8 for melt-through (ϵ). They differ from the probabilities for the B_4 LOCA due to the differences in the timing of the accident phenomenology. The probability for containment leakage (β) for these sequences did not change from the 0.007 value for the B_4S_{23} sequence, however the reduced probabilities of the initiating events resulted in frequencies of less than 1E-7 for these sequences, and this value is below the cutoff value used in the evaluation.

b. Loss of Offsite Power Transient Followed by Failure of Emergency Feedwater, Primary System Makeup, Containment Pressure Reduction and Post Accident Radioactivity Removal (Sequence $T_{2A}T_{10}$; 5.4E-5/yr)

This sequence is initiated by a loss of offsite power followed by the failure of emergency feedwater, failure of the high pressure injection (HPI) system to provide primary system makeup (in the feed-and-breed mode), and failure of both the reactor building spray system (RBSS) and the reactor building cooling system (RBCS). Failure of both the RBSS and RBCS results in failure of the containment pressure reduction and radioactivity removal functions.

In this sequence, the loss of normal AC power results in degraded operating conditions for all of the mitigating systems. Normal secondary heat removal is lost immediately, and the subsequent failure of emergency feedwater results in a condition where no heat is being removed from the reactor and the coolant is being boiled off through the safety/relief valves, with the pressure remaining high. The operator has 20 minutes to manually initiate primary system cooling by feed-and-bleed. Failure of feed-and-bleed results in the eventual uncovering of the core and subsequent core melt. In addition, failure of the RBSS and RBCS results in an inability to remove heat or fission products from the containment atmosphere.

This sequence is the second most dominant contributor to release categories 2, 4 and 6. It contributes about 40% to category 2 when containment failure results from overpressurization, about 45% to category 4 when the release results from containment leakage, and about 35% to category 6 when containment failure results from melt-through.

The number of functional failures involved in this sequence makes it unlikely to occur by combinations of completely independent faults. The common mode of vulnerability in this case lies primarily in the dependence upon emergency AC and DC power. This is readily seen in the three dominant failure modes which are outlined below.

Failure Mode (Cut Set): T_{2A}•A2•A3•DCB (2.3E-5/yr; 43%)

T_{2A} = Initiating Event: Loss of offsite poer (0.32/yr)
A2 = Failure of backup emergency AC power From Crystal River Units 1 and 2 (0.36/demand)
A3 = Failure of diesel A to start and run (6.1E-2/demand)
DCB = Failure of battery B (3.2E-3/demand)

Failure Mode (Cut Set): T_{2A}•A2•A3•A5•E1 (9.6E-6/yr; 18%)

T_{2A}•A2•A3 = Defined above (7.0E-3/yr)
A5 = Failure of diesel B to start and run (6.2E-2/demand)
E1 = Failure of turbine driven emergency feedwater train (2.2E-2/demand)

Failure Mode (Cut Set): T_{2A}•A2•DCB•AM1 (5.9E-6/yr; 11%)

T_{2A}•A2•DCB = Defined above (3.7E-4/yr)
AM1 Diesel train A is unavailable due to test or maintenance (1.6E-2/demand)

Note that failure of the B battery itself fails both the B diesel (the breaker connecting the generator to the bus fails to close) and the turbine driven emergency feedwater pump. With simultaneous failure of the A diesel, the last line of defense against failure of all (secondary, primary, and containment) emergency cooling is the availability of emergency AC power from Unit 1 or Unit 2. The resulting sequence frequency is about three times lower than it would be if the two fossil units weren't at the CR-3 site.

The B diesel and the turbine driven pump could fail independently. This possibility contributes significantly (~18%) to the sequence frequency. At the time of the analysis, the turbine pump itself was dependent upon AC power. The present analysis is based on credit given for removing this dependency.

The failure of post-accident radioactivity removal does not require an additional failure in that it follows functionally from failure of containment pressure reduction.

The failure modes described together contribute about 72% to the sequence frequency. No other single failure mode contributes more than 10%. The containment failure mode probabilities for this sequence are 0.5 for both overpressurization (δ) and melt-through (ε), and 0.007 for containment leakage (β).

This sequence deserves further examination when it is being compared to the similar sequence in the Reactor Safety Study analysis of Surry because the differences are due in part to methodological issues. For example, the two studies use different assumptions regarding the recoverability of off-site power, which could impact the interpretation of this sequence as well as others. The impact of different assumptions (relative to WASH-1400) or specific sequences or specific release categories has not been examined in the Crystal River study.

c. Small-small LOCA Followed by Failure of Reactor Building Spray Recirculation and Emergency Coolant Recirculation (Sequence B_4S_6; 3.9E-6/yr)

This sequence is initiated by a small-small LOCA followed by success of all systems in the injection phase, and failure during the recirculation phase, of both the reactor building spray systems (RBSR) and the high pressure recirculation (HPR) system, which provides emergency coolant to the core. In this sequence, the initial loss of coolant through the break is replenished by emergency coolant injection (ECI) and both the reactor building fans and sprays are available for pressure control. The eventual loss of HPR results in the uncovering of the core, followed by core melt. In addition, loss of the sprays during recirculation results in the inability to remove radioactivity from the containment atmosphere, although containment overpressure is still controlled by the reactor building fans.

This sequence contributes about 3% to category 2 when containment failure results from hydrogen burning and about 3% to category 6 when containment failure results from melt-through.

The frequency of this sequence is estimated as 3.9E-6/yr. The dominant contributors (cut sets) to this frequency are described below:

Failure Mode (Cut Set): B_4•LO4 (3.9E-6/yr; 97%)

B_4 = Initiating Event: Small-small LOCA (1.3E-3/yr)

LO4 = Operator fails to initiate recirculation in time, draining the BWST; pump failure results from insufficient water in the BWST (0.003/demand)

The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ).

d. Loss of Offsite Power Transient Followed by Failure of Emergency Feedwater, Primary System Makeup, and Post Accident Radioactivity Removal (Sequence $T_{2A}T_9$; 2.5E-6/yr)

This sequence is initiated by a loss of offsite power followed by the failure of emergency feedwater, failure of the high pressure injection (HPI) system to provide primary system makeup (in the feed-and-bleed mode), and failure of the reactor building spray system (RBSS), which fails the post-accident radioactivity removal function.

In this sequence, the loss of normal AC power results in degraded operating conditions for all of the mitigating systems. Normal secondary heat removal is lost immediately, and the subsequent failure of emergency feedwater results in a condition where no heat is being removed from the reactor and the coolant is being boiled off through the safety/relief valves, with the pressure remaining high. The operator has 20 minutes to manually initiate primary system cooling by feed-and-bleed. Failure of feed-and-bleed results in the eventual uncovering of the core and subsequent core melt. Thus far, the sequence is identical to sequence $T_{2A}T_{10}$. The sequence differs from $T_{2A}T_{10}$ in that the reactor building cooling system (RBCS) operates successfully, controlling containment overpressure, although the reactor building spray system (RBSS) fails, as it did in sequence $T_{2A}T_{10}$, so that radioactivity is not removed from the containment atmosphere.

The sequence contributes about 2% to releases in category 2 when containment failure results from hydrogen burning, and about 2% to releases in category 6 when containment failure results from melt-through.

The frequency of this sequence is estimated as 2.5E-6/yr. The dominant contributors to this frequency are described below:

Failure Mode (Cut Set): T_{2A}•A2•A3•E1•DM2 (3.3E-7/yr; 13%)

T_{2A} = Initiating Event: Loss of offsite power (0.32/yr)

A2 = Failure of backup AC power from Crystal River units 1 and 2 (0.36/demand)

A3 = Failure of diesel A to start and run (6.1E-2/demand)

E1 = Turbine-driven emergency feedwater pump fails to start or some other fault fails the turbine-driven train (2.2E-2/demand)

DM2 = A component in the decay heat closed cycle cooling system (DHCCCS) train B is out of service for maintenance (2.1E-3/demand)

Failure Mode (Cut Set): T_{2A}•A2•A3•E1•D2 (3.1E-7/yr; 12%)

T_{2A}•A2•A3•E1 Defined above (1.6E-4/yr)

D2 = A hardware fault occurs in the DHCCCS train B (2.0E-3/demand)

These two failure modes contribute about 25% of the risk from this sequence. The remainder is contributed by a number of cut sets which contribute less than 10% each. These other cut sets are made up of various combinations of human and hardware failures of many kinds; no definite pattern is discernable.

The containment failure mode probabilities for hydrogen burning (γ) and melt-through (ϵ) are 0.5 for each, given occurrence of the sequence.

e. Small-Small LOCA Followed by Failure of High Pressure Recirculation (Sequence B_4S_2; 1.7E-4/yr)

This sequence is initiated by a small-small LOCA followed by success of all systems during the emergency coolant injection phase of post-accident operation and failure of high-pressure emergency cooling during the recirculation phase. The initial loss of coolant is replenished by high-pressure emergency coolant injection from the borated water storage tank (BWST). Containment pressure is controlled by the reactor building cooling system (fan coolers) with the reactor building sprays available as needed. This phase lasts about 10 hours, at which time injection water is no longer available from the BWST and the operator must switch manually, by realigning a number of valves, to high pressure recirculation (HPR) from the reactor building sump. The failure of HPR results in the uncovering of the core and eventually the melting of the core.

This sequence dominates release categories 3, 5 and 7. It contributes about 75% to category 3 when containment failure results from hydrogen burning, about 90% to category 5 when containment failure results from leakage, and about 70% to category 7 when containment failure results from melt-through.

The B_4S_2 sequences in release categories 3 and 7 appear to have the highest expected frequency of any of the CR-3 sequences considered. In the context of the IREP objectives, this basic sequence is definitely an outlier with respect to the full spectrum of CR-3 sequences. It is also an outlier relative to the Reactor Safety Study analysis of Surry in the sense that it dominates the probabilities of releases in categories 3 and 7 at CR-3, which are significantly higher than the corresponding earlier estimates for Surry. These observations, however, should be tempered with recognition of the reasons for the higher frequency estimates. To this end, the most important modes of failure for the sequence (exclusive of containment failure) are indicated below:

Failure Mode (Cut Set): B4•H*02 (1.0E-4/yr; 59%)

B4 = Initiating Event: Spontaneous (random) small-small LOCA (1.3E-3/yr)

H*02 = While attempting to switch from high pressure injection to recirculation, operator makes an error in the realignment of valves which fails recirculation (0.08/demand)

Failure Mode (Cut Set): B4•L06 (6.5E-5/yr; 38%)

B4 = Defined above (1.3E-3/yr)

L06 = After having switched to recirculation, an operator shuts down the low pressure pumps, believing they are not needed, since they would already have been shut down three previous times when not needed during injection (0.06/demand)

The sequence probability, given the initiating event, is clearly due almost entirely to two closely related operator faults occurring in the transition from coolant injection to recirculation, and the fact that recovery was not considered in the evaluation. Related faults appear in other sequences as well.

The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ), and 0.007 for containment leakage (β).

f. Loss of Offsite Power Transient Followed by Failure of Emergency Feedwater and Primary System Makeup (Sequence $T_{2A}T_8$; 1.4E-5/yr)

This sequence is initiated by a loss of offsite power followed by the failure of emergency feedwater and failure of the high pressure injection (HPI) system to provide primary system makeup (feed-and-bleed). The loss of normal AC power results in degraded operating conditions for all the mitigating systems. Normal heat removal through the steam generators is lost immediately, and the subsequent failure of emergency feedwater results in a condition where no heat is being removed from the reactor and the coolant is being boiled off through the safety/relief values, with the pressure remaining high. The operator has about 20 minutes to initiate primary system makeup (feed-and-bleed) manually. The failure of feed-and-bleed in this sequence results in a core melt. The containment functions continue to control containment pressure and radioactive effluent releases.

In this sequence, the loss of normal AC power results in degraded operating conditions for all of the mitigating systems. Normal secondary heat removal is lost immediately, and the subsequent failure of emergency feedwater results in a condition where no heat is being removed from the reactor and the coolant is being boiled off through the safety/relief valves, with the pressure remaining high. The operator has 20 minutes to manually initiate primary system cooling by feed-and-bleed. Failure of feed-and-bleed results in the eventual uncovering of the core and subsequent core melt. Thus far, the sequence is identical to sequences $T_{2A}T_{10}$ and $T_{2A}T_9$. This sequence differs from those described earlier in that both the containment cooling and radioactivity removal functions succeed.

This sequence contributes about 6% to category 3 when containment failure results from hydrogen burning, about 8% to category 5 when the release results from containment leakage, and about 6% to category 7 when containment failure results from melt-through.

The frequency of this sequence is estimated as 1.4E-5/yr. The dominant contributors (cut sets) to this frequency are described below:

Failure Mode (Cut Set): $T_{2A}\bullet A2\bullet A3\bullet E1\bullet H4$ (3.1E-6/yr; 22%)

T_{2A} = Initiating Event: Loss of offsite power (0.32/yr)

A2 = Failure of backup AC power from Crystal River units 1 and 2 (0.36/demand)

A3 = Failure of diesel A to start and run (6.1E-2/demand)

E1 = Turbine-driven emergency feedwater pump fails to start or some other fault fails the turbine-driven train (2.2E-2/demand)

H4 = One of two manual valves in high pressure injection train B is left closed (2.0E-2/demand)

Failure Mode (Cut Set): $T_{2A}\bullet A2\bullet A3\bullet E1\bullet H03$ (2.2E-6/yr; 16%)

$T_{2A}\bullet A2\bullet A3\bullet E1$ Defined above (1.6E-4/yr)

H03 = Operator fails to correctly observe and diagnose the need for feed-and-bleed and therefore does not initiate it (1.4E-2/demand).

These two failure modes contribute about 38% of the risk from this sequence. No other one failure mode contributes more than 10%.

The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ), and 0.007 for containment leakage (β).

The essential difference between this sequence and the $T_{2A}T_{10}$ sequence discussed earlier is that in the latter, both post-accident heat and radioactivity removal from containment fail, whereas here they both succeed.

g. Small-small LOCA Followed by Failure of Emergency Coolant Injection (Sequence B_4S_9; 9.0E-6/yr.)

This sequence is initiated by a small-small LOCA followed by failure of the emergency coolant injection (ECI) system, which for this size break is the high pressure injection (HPI) system. The initial loss of coolant through the break is not replenished due to the loss of ECI (HPI) at some time during the injection phase of the accident. This results in the eventual uncovering of the core and subsequent core melt. The reactor building fans and sprays are available to control containment overpressure and remove radioactivity from the containment atmosphere.

This sequence contributes about 4% to category 3 when containment failure results from hydrogen burning, and about 4% to category 7 when containment failure results from melt-through.

The frequency of this sequence is estimated as 9.0E-6/yr. The dominant contributors (cut sets) to this frequency are described below:

Failure Mode (Cut Set): B_4•H01 (5.2E-6/yr; 58%)

B_4 = Initiating Event: Small-small LOCA (1.3E-3/yr)

H01 = Operator shuts down the HPI system prematurely, believing that it is no longer required (0.004/demand)

This failure mode contributes about 58% of the risk from this sequence. The remainder is contributed by a number of cut sets which contribute less than 10% each.

The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ).

h. Loss of Power Conversion System Transient Followed by Failure of Emergency Feedwater and Primary System Makeup (Sequence $(T_2\text{-}T_{2A})T_8$; 8.6E-6/yr)

This sequence is initiated by a loss of power conversion system (PCS) transient not caused by loss of offsite power, followed by failure of emergency feedwater and failure of the high pressure injection (HPI) system to provide primary system makeup (feed-and-bleed). The loss of PCS results in the immediate loss of normal heat removal. The subsequent failure of emergency feedwater results in a condition where no heat is being removed from the reactor and the coolant is being boiled off through the safety/relief valves, with the pressure remaining high. The operator has 20 minutes to initiate primary system (feed-and-bleed) manually. The failure of feed-and-bleed in this sequence results in a core melt. The containment functions continue to control containment pressure and radioactive effluent releases.

This sequence contributes about 4% to category 3 when containment failure results from hydrogen burning, and about 4% to category 7 when containment failure results from melt-through.

The frequency of this sequence is estimated as 8.6E-6/yr. The dominant contributors (cut sets) to this frequency are described below:

Failure Mode (Cut Set): (T_2-T_{2A})•E1•EM2•H03 (3.0E-6/yr; 35%)

T_2-T_{2A} = Initiating Event: Loss of power conversion system transient, not caused by loss of offsite power (1.78/yr)

E1 = Turbine-driven emergency feedwater pump fails to start or some other hardware fault fails turbine-driven train (2.2E-2/demand)

EM2 = A component in the motor-driven emergency feedwater pump train is out of service for test or maintenance (5.5E-3/demand)

H03 = Operator fails to correctly observe and diagnose the need for feed-and-bleed and therefore does not initiate it (1.4E-2/demand).

Failure Mode (Cut Set): (T_2-T_{2A})•E01•H03 (2.5E-6/yr; 29%)

(T_2-T_{2A})•H03 Defined above (2.5E-2/yr)

E01 = Auto actuation system for the emergency feedwater system is locked out and the operator fails to recover it (1E-4/demand)

Failure Mode (Cut Set): (T_2-T_{2A})•E1•E2•H03 (1.9E-6/yr; 22%)

(T_2-T_{2A})•E1•H03 Defined above (5.5E-4/yr)

E2 = Motor-driven emergency feedwater pump fails to start or some other hardware fault fails motor-driven train (3.5E-3/demand)

These three failure modes contribute about 86% of the risk from this sequence. The remainder is contributed by a number of cut sets which contribute less than 10% each.

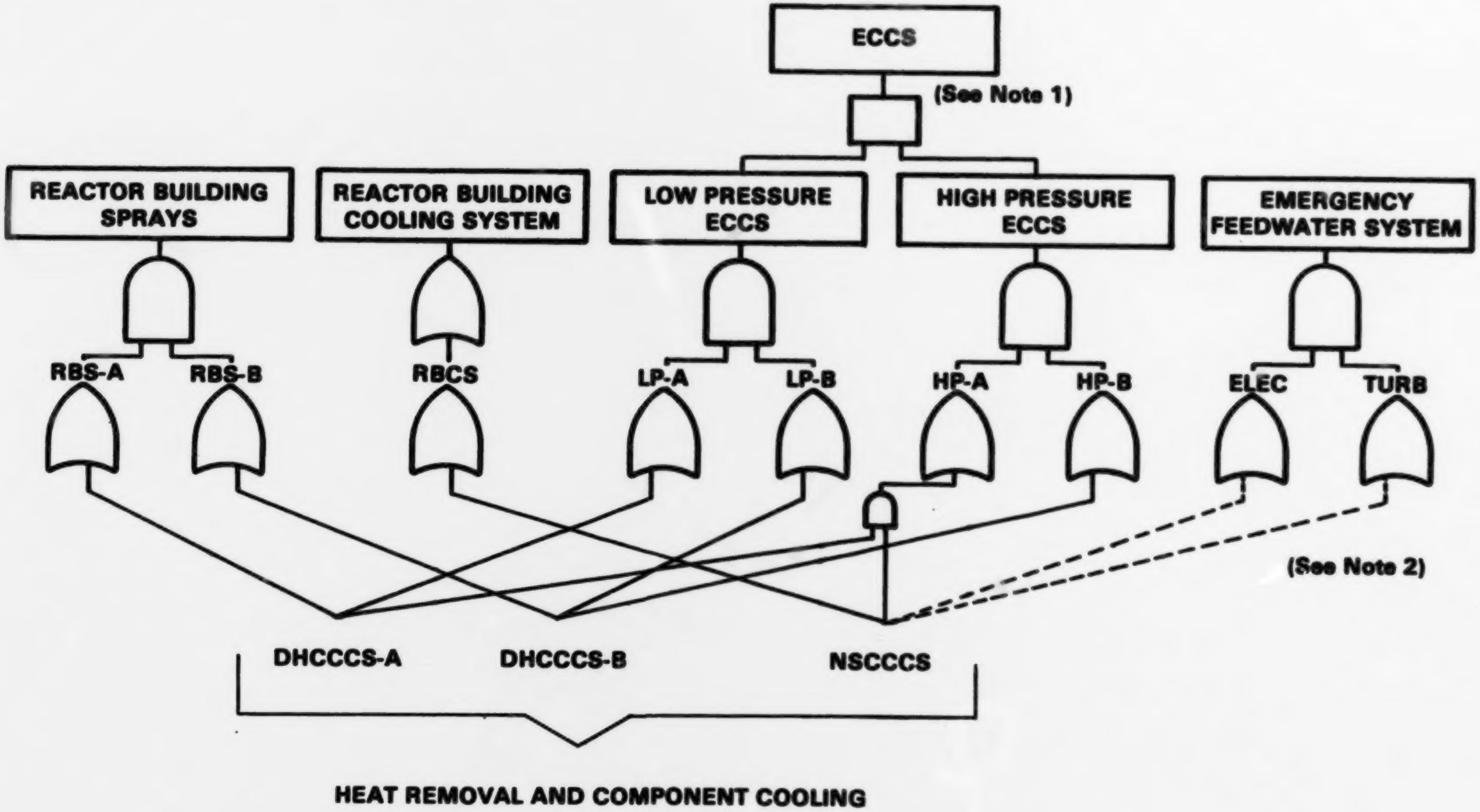
The containment failure mode probabilities for this sequence are 0.5 for both hydrogen burning (γ) and melt-through (ϵ).

2.3 Functional and System Dependencies

It was noticed very early in the study that CR-3 appeared to have more interconnections between safety (and support) systems than observed in Surry-1, the plant analyzed in WASH-1400. This observation, and a desire to be able to clearly describe the interdependencies, led to the development of "system interaction diagrams." These diagrams provide a tool for rapidly understanding and communicating the logical structure of plant systems and their dependencies on various support systems.

Two diagrams constructed for CR-3 are presented in Figures 2.2 and 2.3. Figure 2.2 illustrates the dependencies that exist at CR-3 between important "front-line" plant systems and the support systems which provide component and heat removal to the front-line systems. Figure 2.3 is the same as the first figure, but with the emergency electric power dependencies superimposed on it. Examination of Figure 2.3 shows, for example, that the "A" Train of the reactor building spray system (RBS-A) is dependent on the "A" Train of the decay heat closed cycle cooling water system and 4160 VAC bus A. Failure of either will fail RBS-A. Other dependencies can be similarly read from the figure. It is also possible to extend this figure to show the electric power dependencies on the diesels, etc.

The extensive interconnections that can be observed in these figures might have been expected to result in risk from the plant being dominated by cooling system dependencies. It is noteworthy that risk is dominated by accident sequences initiated by small-small LOCAs and loss of offsite power, as described in Section 2.1. The loss of offsite power initiating event results in a relatively high probability of losing both of the 4160 VAC buses because of the high failure rate for the diesel generators providing emergency back-up power to the buses.


ECCS
(See Note 1)
REACTOR BUILDING SPRAYS
REACTOR BUILDING COOLING SYSTEM
LOW PRESSURE ECCS
HIGH PRESSURE ECCS
EMERGENCY FEEDWATER SYSTEM
RBS-A
RBS-B
RBCS
LP-A
LP-B
HP-A
HP-B
ELEC
TURB
(See Note 2)
DHCCCS-A
DHCCCS-B
NSCCCS
HEAT REMOVAL AND COMPONENT COOLING

NOTES:

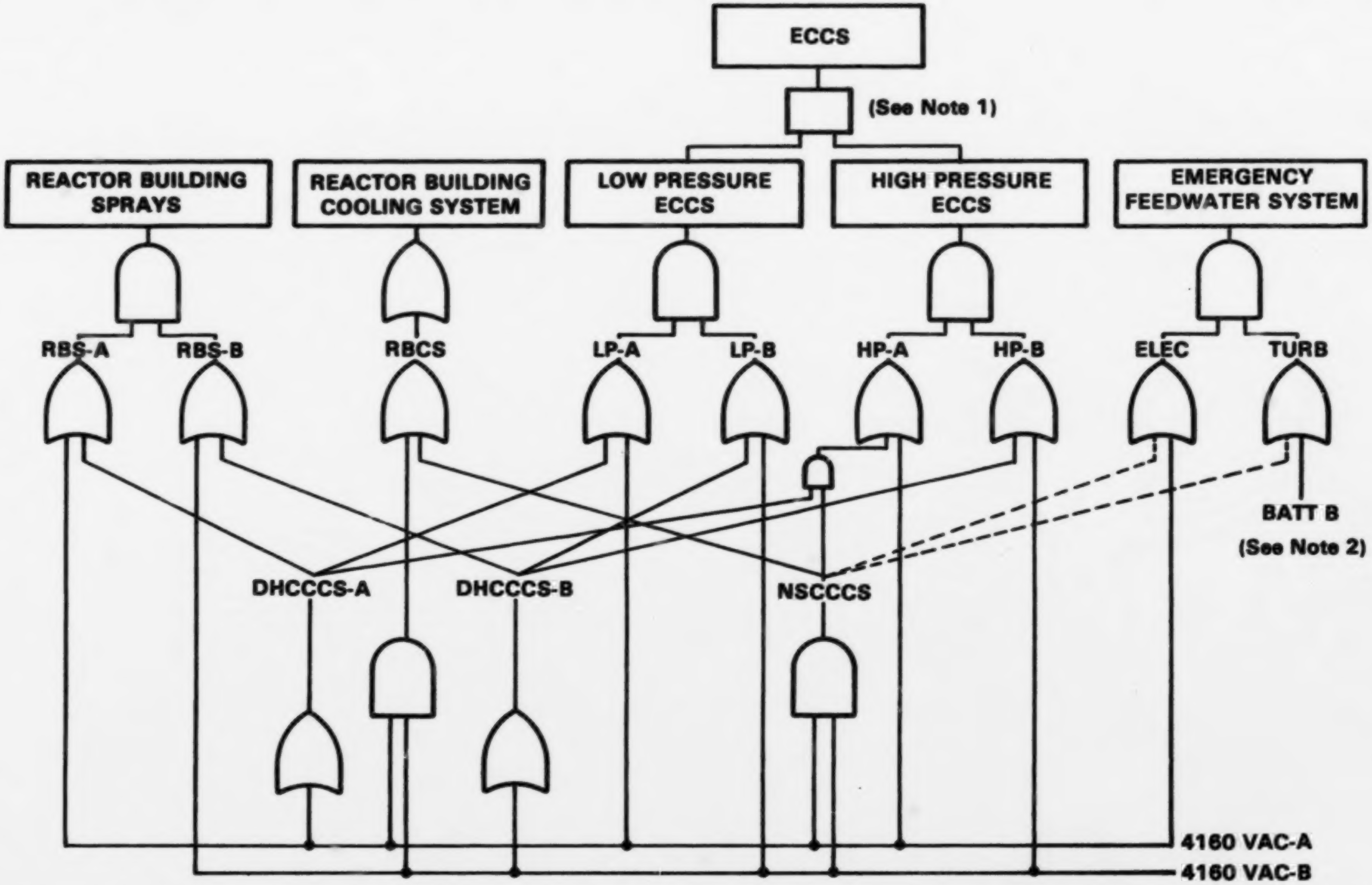
1. Logic depends on LOCA size.
2. The dashed lines indicate existing dependencies in Crystal River-3 which Florida Power Corporation has committed to remove.

LEGEND:

— AND Gate: All inputs must fail to fail output

— OR Gate: Any input failing will fail output

FIGURE 2.2. DEPENDENCIES ON EMERGENCY COOLING SYSTEMS IN CRYSTAL RIVER-3


ECCS
(See Note 1)
REACTOR BUILDING SPRAYS
REACTOR BUILDING COOLING SYSTEM
LOW PRESSURE ECCS
HIGH PRESSURE ECCS
EMERGENCY FEEDWATER SYSTEM
RBS-A
RBS-B
RBCS
LP-A
LP-B
HP-A
HP-B
ELEC
TURB
BATT B
(See Note 2)
DHCCCS-A
DHCCCS-B
NSCCCS
4160 VAC-A
4160 VAC-B

NOTES:

1. Logic depends on LOCA size.
2. The dashed lines indicate existing dependencies in Crystal River-3 which Florida Power Corporation has committed to remove.

LEGEND:

— AND Gate: All inputs must fail to fail output

— OR Gate: Any input failing will fail output

FIGURE 2.3. DEPENDENCIES ON EMERGENCY ELECTRIC POWER AND COOLING SYSTEMS IN CRYSTAL RIVER-3

Figure 2.4 shows the system interactions among AC power, DC power Train B, and EFS for one of the dominant sequences in release category 2. This system interaction diagram suggests several options for reducing the frequency of transient-initiated dominant sequences in the low-numbered, high-consequence release categories. Three such options are:[1]

A. Reconfigure DC power to the EFS steam admission valve so that the valve can be powered from either DC power train.

B. Replace (or parallel) the present steam admission valve with an air operated valve which fails open on loss of control DC power.

C. Provide the EFS with a redundant turbine pump. Steam feed to this pump is provided through a new steam admission valve powered by the opposite ("A") DC train.

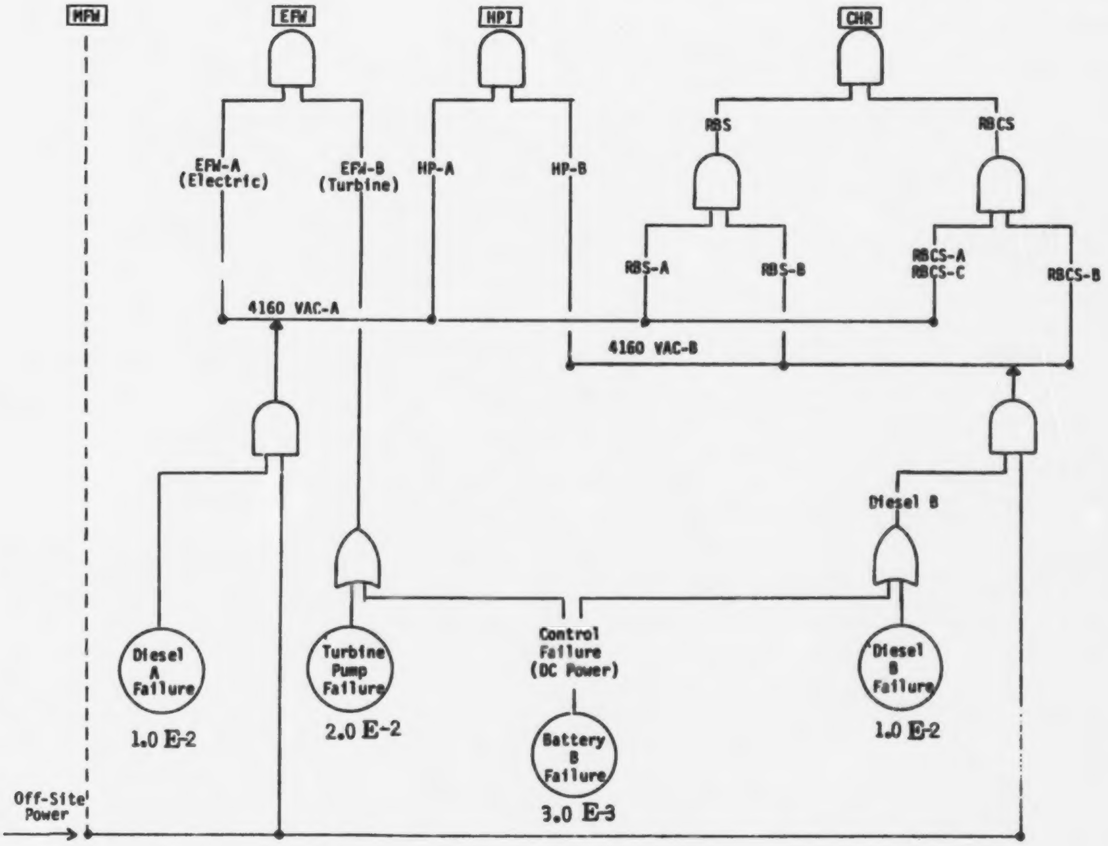
Option A would remove the dependence of the turbine-driven pump train on a single DC power train; this would result in about a factor of two reduction in the sequence point estimates. This factor of two reduction would apply to many of the dominant transient-initiated sequences in the high release categories. It would, of course, be necessary to verify that such a system modification did not also result in an unacceptable side effect, such as a significant increase in the probability of a (common-cause) failure of both DC trains.

Option B would remove the dependence of the turbine-driven pump train on DC power. This would have essentially the same effect as Option A.

Option C would remove the dependence of the turbine system on a single DC power train and also remove EFS dependence on a single turbine-driven pump during a loss of all AC power. This should result in a reduction of risk by a factor of ten or more.

---

[1] A fourth option might consider designs that would, on loss of control DC power, automatically provide steam to the turbine-driven EFP from the hot steam line that runs from CR-1 and CR-2 to CR-3. No credit was given for this potential steam supply in the present analysis because the control valve is manually operated.


MFW
EFW
HPI
CHR
RBS
RBCS
EFW-A (Electric)
EFW-B (Turbine)
HP-A
HP-B
RBS-A
RBS-B
RBCS-A
RBCS-C
RBCS-B
4160 VAC-A
4160 VAC-B
Diesel B
Diesel A Failure
1.0 E-2
Turbine Pump Failure
2.0 E-2
Control Failure (DC Power)
Battery B Failure
3.0 E-3
Diesel B Failure
1.0 E-2
Off-Site Power

Initiator: Loss of Offsite Power

Figure 2.4 System Interactions and Dominant Contributors to One of the Crystal River-3 Dominant Sequences ($T_{2A}T_{10}$)

A quantitative evaluation of the actual probability reductions which would result from these options (or combinations thereof) was not within the scope of the study. It is suggested that such an evaluation be performed prior to making any changes to the system design so that both the positive and negative aspects of potential changes can be carefully considered. It is also suggested that other options considered for potential risk reduction be similarly evaluated. Such evaluations would provide a basis for a cost-benefit comparison of the various options.

2.4 Limitations of the Analysis

The applicability of the results of this analysis is circumscribed by the important limitations indicated in the Introduction; these are (1) the restricted set of initiating events, (2) the use of a surrogate measure of risk in lieu of estimating consequences, and (3) the use of point estimates without an accompanying analysis of uncertainties.

The most important exclusions from the set of initiating events are natural disasters such as earthquakes and tornados and any other events having comparable potential for causing widespread damage to the plant. The representation of risk in terms of radioactivity releases essentially removes any influence of site characteristics (meteorological and demographic) on the results. It helps to focus specifically on the operational reliability of the systems designed to mitigate accidents of low to moderate frequency; it makes the results more generic (applicable to plants other than CR-3) than they would if consequences were considered, although the analysis is highly specific to the CR-3 system design. In any case, the first two limitations indicated are fully consistent with the objective of identifying risk "outliers" associated with system design and reliability.

The use of point estimates means that no formal statistical interpretation can be given to the results. The estimated probabilities may simply be thought of as "best estimates", with the notion of best in this context represented by its intuitive, everyday, nontechnical meaning. The lack of an uncertainty analysis means that there is no basis for associating a level of confidence with the likelihood that a design decision relating to risk would have its intended effect. This limitation is somewhat more serious than a simple restriction of scope in that it lessens the usefulness of the results even in a domain where they are applicable. The objective of identifying significant risk problems should be taken very literally; the results may yield suggestions but they are not sufficient to say for sure what to do about the problems identified. It might be noted in passing, however, that nearly all the information necessary to perform a comprehensive sensitivity analysis is contained in this report and its supporting appendices.

As already indicated the technical safety issues associated with the OTSG and the ICS were the subject of the second major objective of the larger CR-3 study. Nevertheless, brief attention was given to the likelihood that faults within the ICS itself could cause an overcooling transient because this problem is at least partially amenable to the fault tree analysis methodology used in the mainstream of this project. It was found, however, that a superficial analysis would not likely be useful and an indepth study was definitely out of scope. Hence, the problem is not addressed in this report except in a passing comment or two.

Several technical issues were important to the analytical framework employed but their investigation would have exceeded the time and resources available. Consequently, it was mutually agreed among sponsors and participants that certain information relating to the Surry and Oconee plants would be taken directly from, respectively, the Reactor Safety Study report (2-1), and the RSSMAP Oconee report (2-2), and adapted to the CR-3 analysis. This information concerned the description of radioactivity release categories, the analysis of containment failure modes, and the component failure rate data base.

The Surry event tree for containment failure (given core melt) was used directly without modification. The release category descriptions were also used directly, even though they originated in a plant-specific analysis of Surrey and are not necessarily the most appropriate for CR-3. The correlation between release categories and the combinations of accident sequences and containment failures modes is based on qualitative identification of the CR-3 sequences with the "nearest" Oconee sequences and reliance on the assignments made in the earlier study. The probabilities of the various containment failure modes were taken directly from the Oconee report, as these are more current and more directly applicable to CR-3. This procedure is used on the tacit assumption that one pressurized water reactor is more or less representative of another as far as containment failure and radioactivity release phenomena are concerned. We believe this assumption is acceptable in view of the limited objectives of the study and the inherent uncertainties from other sources.

The basic component reliability data base used is identical to that used in the Reactor Safety Study, except that the failure rates associated with safety relief valves and with turbine-driven pumps have been changed. This might be considered a minor limitation in that six years of data collection activities have transpired in the interim. However, the same data has been adopted as the official data base for Phase II of IREP (2-3), so there is no significant limitation within the context of that program. In a few instances, we went beyond the original scope of the study and examined data specific to CR-3 and to B&W plants. The most significant consequence was the elimination of "coupling" between the two emergency diesel-generators with regard to their failure to start.

In connection with the coupling phenomenon in general, the CR-3 analysis treats most common mode failures in terms of a conditional probability of a second failure, given the first; the conditional probability is represented by a "β factor." This approach is in contrast to the much-criticized bounding technique used in the Reactor Safety Study. It is recognized, however, that the change in formalism does not lessen the need for data related to common mode failures, of which there is very little. For all active components that are assumed to be subject to coupling, the value of β is generally assumed to be 0.1. There is some information to support this (2-4, 2-5) and there seems to be a loose concensus in the probabilistic risk assessment community that this value is about right. The β factors would be prime candidates for attention in a sensitivity analysis. Nevertheless, the "β factor approach" to coupling is not an inherent limitation of the study, any more so than any other source of uncertainty.

The plant was analyzed in the "as built" configuration as of November 1979, except that modifications arising from post-TMI regulations for which the utility had made a commitment to complete by the end of the next scheduled refueling outage were included.[1]

A number of specific technical assumptions of a rather detailed nature are worthy of mention, even though they are entirely consistent with normal practice in previous probabilistic risk assessment studies.

We note first that system reliabilities are evaluated for only a period of 24-hours following postulated accidents, even though the core may have to be cooled for months (as in TMI-2). This feature of the analysis is adopted for several reasons. The functional, and therefore equipment, success requirements are much reduced after the first 24-hours so systems in effect become more redundant; greater downtime intervals can be tolerated; there is greater opportunity for repair and recovery of a least some equipment. In general, there is greater likelihood that alternative success paths can be improvised if necessary after 24-hours. In effect, we assume that the probability of system failure, given successful operation for the first 24-hours, is small in relation to the probability of failure-to-start and to operate successfully for 24-hours. This assumption has been common since the Reactor Safety Study, and while we have not sought to verify its validity, we believe it to be acceptable from a quantitative viewpoint.

Within the 24-hour period following accident initiation, no credit is taken for repair and recovery of failed equipment. In addition, equipment out-of-service for maintenance is assumed not to be recoverable in the first 24-hours. Test outages, however, are generally assumed to be reversible, which means they do not contribute to system unavailability.

No credit is given for operator actions not called for in a written procedure, i.e., for the possibility of an operator coming up with a novel or imaginative (but nonstandard) method of mitigating an accident; nor was credit given for operator errors acting fortuitously to improve the situation (the "no miracle rule"). On the other hand, credit was generally given for standard operator actions from the control room to manually actuate a system whose auto-actuation failed.

---

[1] An example of a modification important to the evaluation is the removal of a dependency of the turbine-driven emergency feedwater pump on cooling water provided by an AC powered system.

In the case of loss-of-offsite-power transients which progress to LOCAs, we have assumed that offsite power is restored by the time the cooling systems must be switched to a recirculation mode of operation. The significance of this is that a single train of a cooling system could be unavailable for coolant injection because of diesel failure and still be available during recirculation. The injection period would likely exceed 10 hours; we feel the likelihood of recovering offsite power in this period is high, but we have little data to support this contention. It might be of interest, however, that the Florida Power Corporation grid appears to be more stable than might be expected for the entire Florida peninsula.

In general, it is assumed that the plant is operated in accordance with the Technical Specifications which are a part of its operating license. In other words, no explicit contributions to system unavailabilities were assessed because of willful violations of technical specifications, e.g., for deliberately exceeding an allowed outage time for a safety system component. While such violations may occur from time to time, there is no data to support an estimate of their contributions, which are probably negligible anyway. The general level of uncertainty places an upper limit on the depth to which the analysis should go. This level is not well-defined, but intentional violations of technical specifications are below it in this case.

As a general rule, the principle that probabilistic risk assessments should attempt to be realistic is followed. Some conservatism inevitably creeps in, however. For example, the sequences for which there is much uncertainty about whether they will proceed to core melt are assumed to do so. On the other hand, some sequences which would almost certainly lead to some core damage are assumed not to lead to core melt. Specific instances are discussed in connection with event tree construction (Chapter 4). In most cases, these types of uncertainties are not quantitatively significant because major releases of radioactivity are most likely to stem from sequences in which there is no doubt that the core will melt.

Conservatism also enters to a minor extent at the component fault level. When data is lacking, faults are often assigned probabilities believed to be conservatively high. Most often, these situations are quantitatively insignificant. If they do turn out to be significant, e.g., if they are important contributors to quantitatively important sequences, the probability estimates are refined through further analytical attention and the sequences are evaluated again. This occurred on several occasions with operator faults. (See, for example, Section 5.4.)

A final comment on limitations concerns the inevitable comparisons between the CR-3 results presented here and the results for Surry-1 from the Reactor Safety Study (indeed, such comparisons are inherent to IREP objectives). Suffice it to note that nearly five years ensued from the end of one study to the beginning of the other. Among the things which have changed are some analytical techniques and some quantitative information. To cite two examples: the two studies treated common mode failures differently; and, the frequency of component outages (for maintenance) at CR-3 is assumed realistically to be about an order of magnitude less than was assumed at Surry, and maintenance outage contributions were significant for Surry. These differences mean that apparent differences between the two reactors could be attributed, to an unknown extent, to differences in analysis rather than in fact. This problem, common to all IREP analyses, could best be alleviated by appropriate uncertainty and sensitivity analysis.

References

2-1 U.S. Nuclear Regulatory Commission, "Reactor Safety Study--An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/104), October 1975.

2-2 C.J. Kolb, S.W. Hatch, P. Cybulskis and R.O. Wooton, Sandia National Laboratories, "Reactor Safety Study Methodology Applications Program: Oconee No 3 PWR Power Plant," USNRC Report NUREG/CR-1659 (2 of 4) January 1981, Revised May 1981.

2-3 Letter from Joseph Murphy, NRC, to David Carlson, Sandia National Laboratories, Subject: Component Failure Rates to be used for IREP Quantification, September 26, 1980.

2-4 D.M. Rasmuson, G.R. Burdick, and J.R. Wilson, EG&G Idaho, Inc., "Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation," Report No. TREE-1349, September 1979.

2-5 C.J. Atwood, Idaho National Engineering Laboratory, "Common Cause and Individual Failure and Fault Rates for Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants-Draft," Report No. EGG-EA-5289, November 1980.

3.0 GENERAL PLANT DESCRIPTION

The Crystal River Unit 3 (CR-3) Nuclear Generating Plant (USNRC Docket No. 50-302) is operated and 90% owned by Florida Power Corporation. The unit is located on the Gulf of Mexico 70 miles north of Tampa and seven miles northwest of Crystal River, Florida, and shares the site with two coal-fired power plants, Crystal River Units 1 and 2, as shown in the site layout plant in Figure 3.1. Unit 3 is a pressurized water reactor (PWR), supplied by the Babcock & Wilcox Company (B&W). The architect-engineer is Gilbert Associates, Inc. The unit is operated at core power levels up to 2452 MWth which corresponds to a gross electrical output of about 855 MWe. The plant was declared commercial in March of 1977. The description of CR-3 presented herein is taken primarily from the Final Safety Analysis Report (3-1).

The reactor building is a dry-type containment[1] structure consisting of a prestressed post-tensioned reinforced concrete cylinder and dome on a conventional reinforced concrete slab, with a steel liner. The design pressure is 55 psig. The containment is similar to those at Arkansas-1; Oconee-1, 2, and 3; Palisades; Point Beach-1 and 2; Three Mile Island-1 and 2, and Turkey Point-3 and 4. Cross sections through the reactor and auxiliary building and through the reactor and spent fuel building are shown in Figures 3.2a and b, respectively.

The B&W nuclear steam supply system (NSSS) has two steam generators and four reactor coolant pumps arranged in two heat transport loops, as shown in Figure 3.3. The NSSS is similar to those at Oconee and Three Mile Island.

---

[1] The terms 'reactor building' and 'containment' are used interchangeably.

BEST DOCUMENT AVAILABLE

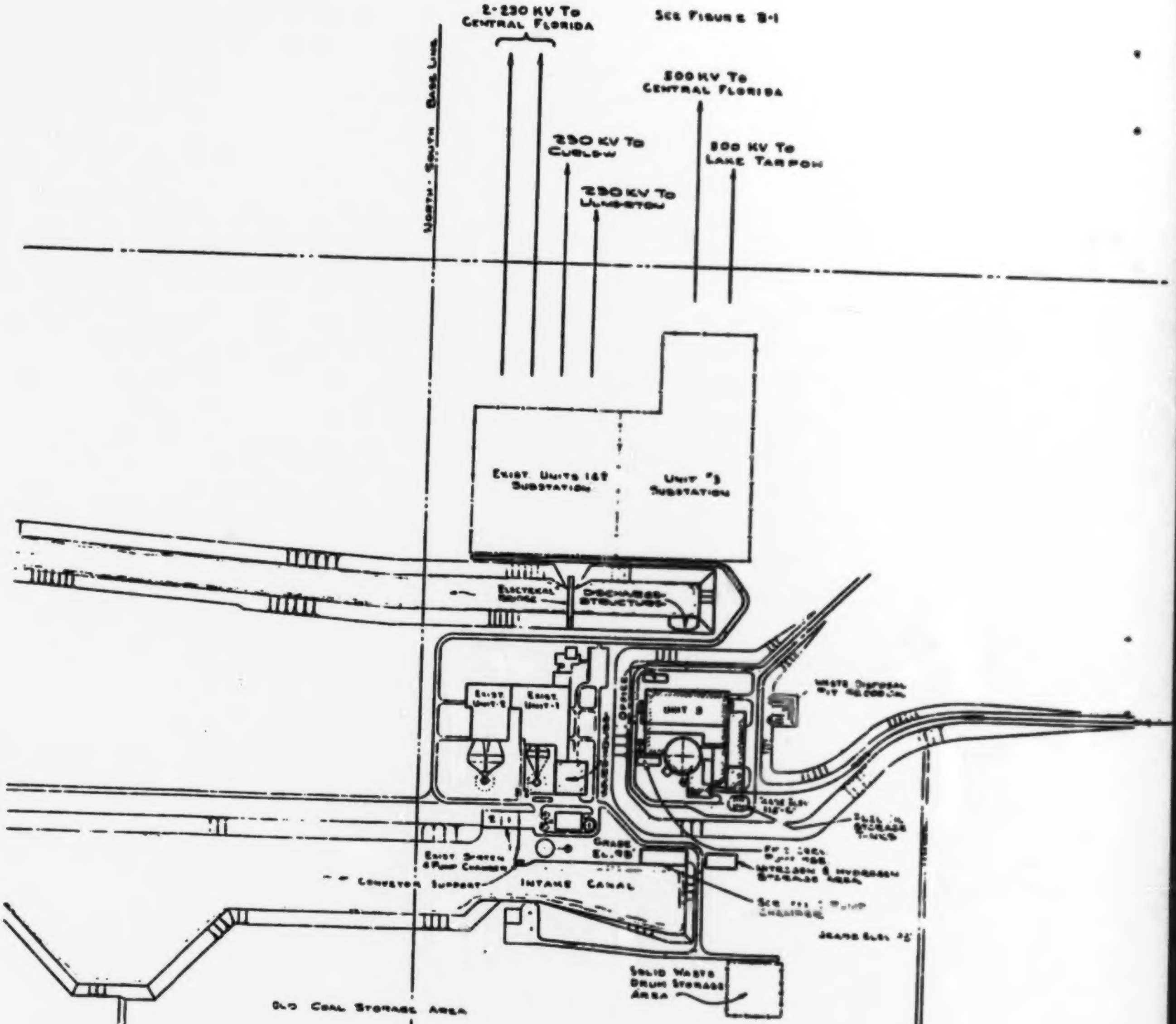

2-230 KV To Central Florida
See Figure 3-1
North - South Base Line
500 KV To Central Florida
230 KV To Curlew
500 KV To Lake Tarpon
230 KV To Ulmerton
Exist. Units 1&2 Substation
Unit #3 Substation
Electrical Bridge
Discharge Structure
Exist. Unit-2
Exist. Unit-1
Offices
Unit 3
Waste Disposal Pit
Fuel Oil Storage Tanks
Grade El.
Exist. Screen & Pump Chamber
Conveyor Support
Intake Canal
Nitrogen & Hydrogen Storage Area
Solid Waste Drum Storage Area
Old Coal Storage Area
Meteorological Building & Tower

Figure 3.1 CR-3 Site Layout Plan
Source: CR-3 FSAR

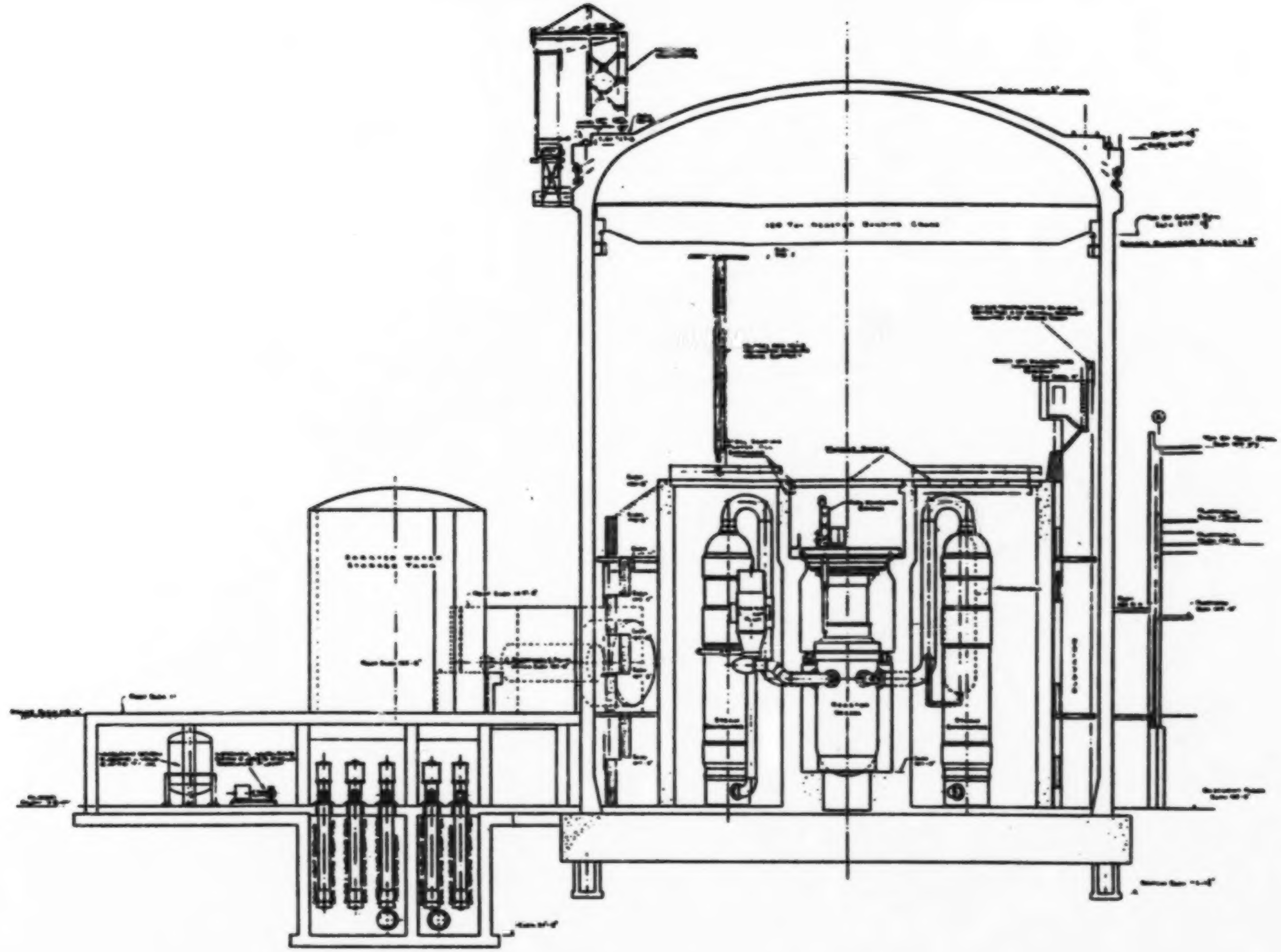


Figure 3.2a Cross Section-Reactor Building and Auxiliary Building
Source: CR-3 FSAR

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

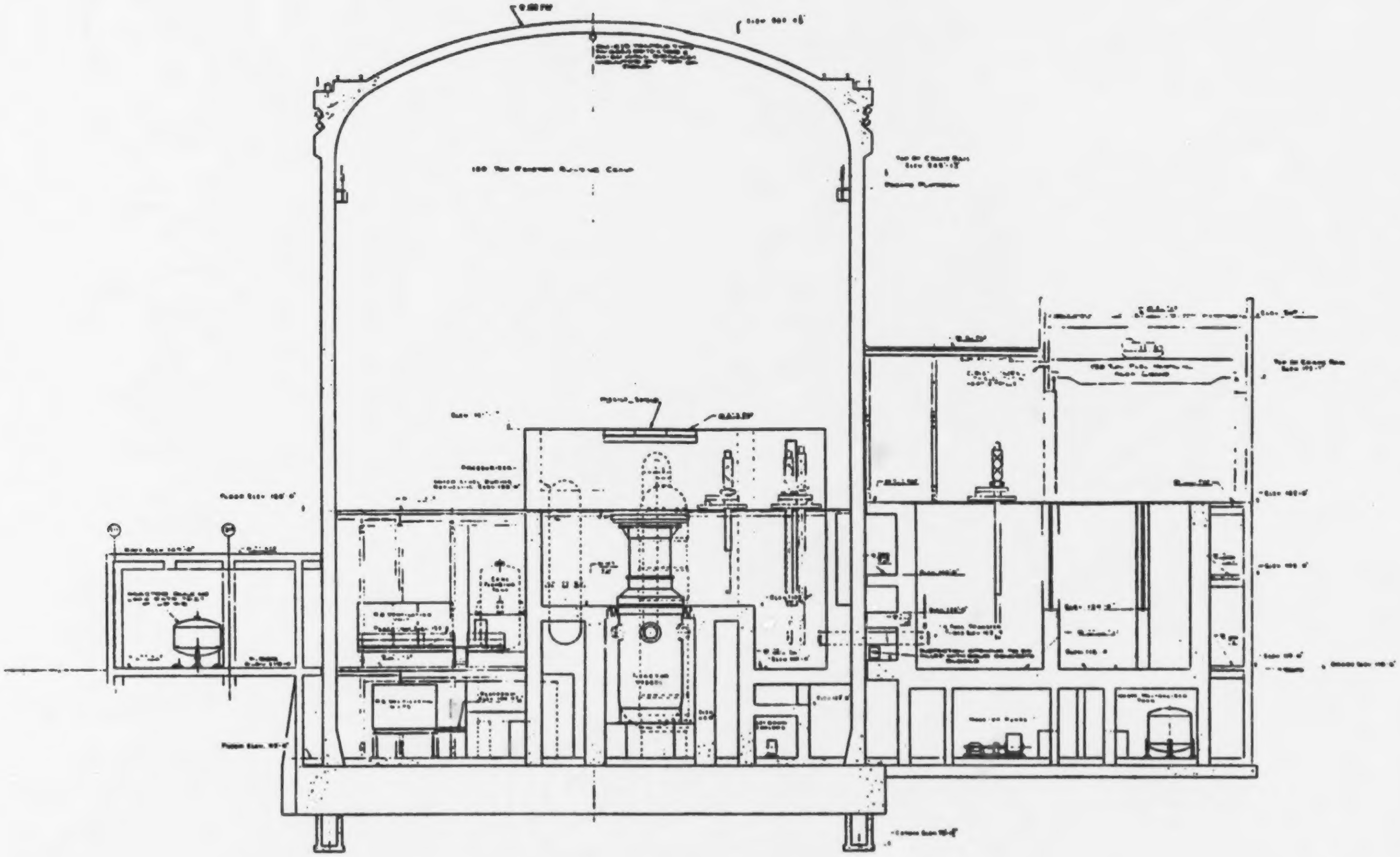


Figure 3.2b Longitudinal Section-Reactor Building and Spent Fuel Building
Source: CR-3 FSAR

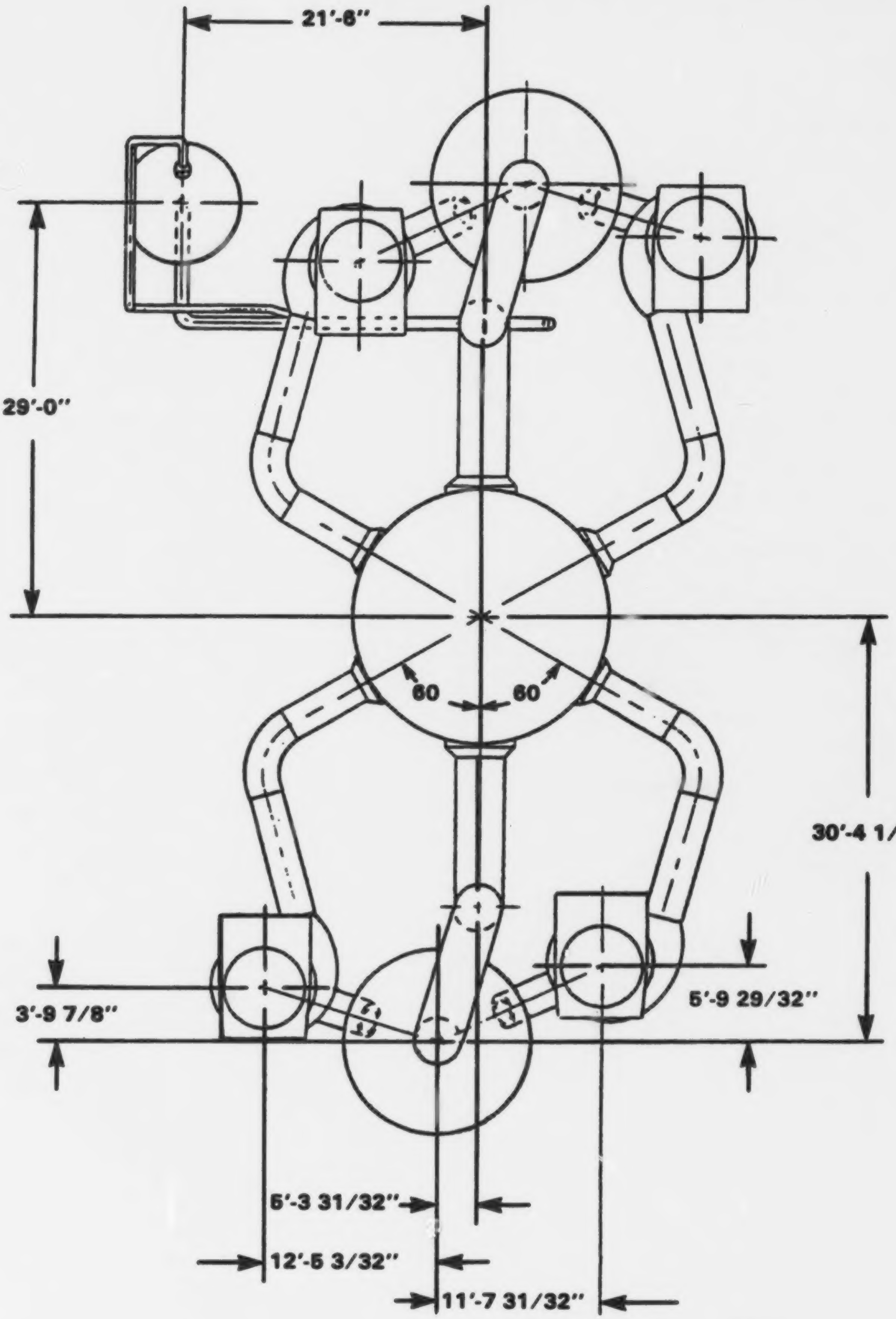

21'-8"
29'-0"
60
60
30'-4 1/2"
3'-9 7/8"
5'-9 29/32"
5'-3 31/32"
12'-5 3/32"
11'-7 31/32"

FIGURE 3.3. REACTOR COOLANT SYSTEM ARRANGEMENT PLAN

The major plant systems required to mitigate the consequences of an accident are listed below:

- Reactor Coolant System
- Reactor Protection System
- Engineered Safeguard Systems
- Emergency Feedwater System
- Emergency Electric Power
- Emergency Cooling Systems

Brief descriptions of each of these systems, and the connections between the nuclear and coal-fired units, are contained in the following sections. Detailed descriptions of these systems are provided in the Appendices to this report.

3.1 REACTOR COOLANT SYSTEM (RCS)

The RCS consists of the reactor vessel, two vertical once-through steam generators (OTSG), four shaft-sealed reactor coolant pumps, an electrically heated pressurizer, and interconnecting piping. The system is arranged in two heat transport loops, each with one OTSG and two reactor coolant pumps. The RCS arrangement plan is shown in Figure 3.3.

The OTSG is a vertical, straight tube and shell heat exchanger which produces superheated steam at constant pressure over the power range. Reactor coolant flows downward through the tubes and transfers heat to generate steam on the shell side. Feedwater is supplied to the shell side (the secondary side) of the OTSG through a feedwater ring located at the side of the steam generator. Natural circulation of the reactor coolant following a loss of all reactor coolant circulating pumps is assured. The OTSG provides a barrier to prevent fission products and activated corrosion products from entering the secondary side.

3.2 REACTOR PROTECTION SYSTEM (RPS)

The Reactor Protection System monitors parameters related to reactor operation and trips the reactor by inserting control rods into the core to protect the core against fuel rod cladding damage. In addition, it protects against reactor coolant system damage from high system pressure.

The RPS consists of control rod assemblies (CRA), circuit breakers, instrumentation, and electronic trip logic. The RPS trip logic includes four identical channels, each consisting of logic circuits and trip relays, which maintain the trip breakers and contactors energized under normal operating conditions. In response to input signals from sensors, the channel logic deenergizes associated trip relays which in turn deenergize the trip breakers and contactors. When any 2-out-of-4 channels trip, all trip breakers and contactors are deenergized. Thus, power from the drive motors is removed and the regulating and safety CRAs drop into the core under the influence of gravity.

3.3 ENGINEERED SAFEGUARDS ACTUATION SYSTEM (ESAS)

The ESAS monitors reactor coolant pressure and reactor building pressure to detect loss of reactor coolant system pressure boundary integrity. Setpoints of 1,500 psig and 500 psig in the RCS, and 4 psig and 30 psig in the reactor building are used to initiate the operation of the High Pressure Injection (HPI), Low Pressure Injection (LPI), Reactor Building Isolation and Cooling (RBIC), and Reactor Building Spray (RBS) Systems. The ESAS also starts engineered safeguards diesel generators A and B.

The ESAS utilizes a 2-out-of-3 redundancy for the detection of "out of limit" conditions and generates redundant actuation signals to control the two trains of engineered safeguards auxiliaries. The redundant outputs are labeled engineered safeguard actuation "A" and "B".

The automatic actuation of the engineered safeguards is backed up by manual actuation switches located in the control room.

3.4 ENGINEERED SAFEGUARDS SYSTEMS

The engineered safeguard systems are designed to mitigate the consequences of an accident by minimizing the release of fission products.

The safeguard systems can be divided into two groups. The first, the Emergency Core Cooling System (ECCS), provides emergency coolant if reactor coolant is lost to ensure that the reactor core is not uncovered and that residual shutdown decay heat is removed. The second group consists of the Reactor Building Emergency Cooling System (RBECS) and the Reactor Building Spray System (RBSS). These two systems are designed to reduce the post-LOCA atmospheric containment pressure, so that the integrity of the reactor building is maintained. The RBSS serves also to remove radioactive iodine fission products from the containment atmosphere.

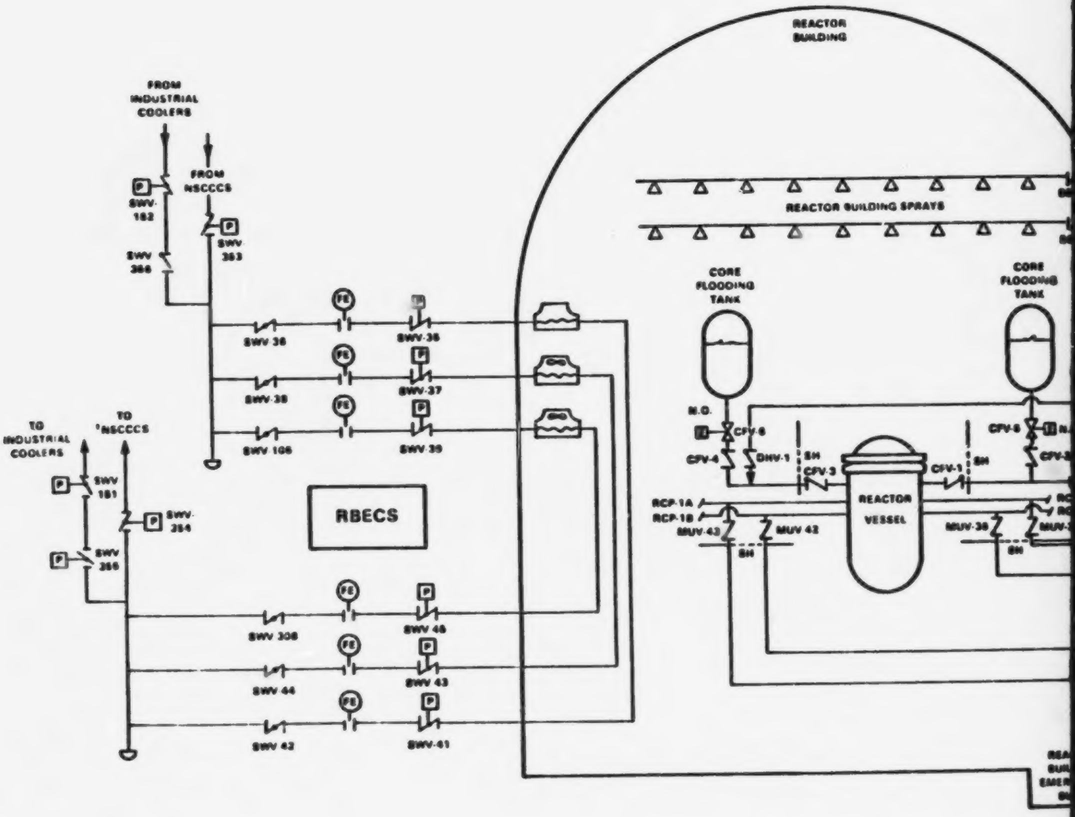
A simplified schematic piping diagram of the engineered safeguard systems is shown in Figure 3.4.

3.4.1 Emergency Core Cooling System (ECCS)

The ECCS consists of the High Pressure (HP), the Low Pressure (LP), and the Core Flood Tank (CFT) Systems. The three systems are designed to cover the entire spectrum of RCS break sizes. They are redundant two-train systems. A portion of each Low Pressure Injection (LPI) train is shared with one Core Flood Tank.

High Pressure Injection (HPI)

The high pressure system operating in the injection mode (HPI) for small LOCAs where a high RCS pressure is maintained and to delay the uncovering of the core for intermediate break sizes. The HPI system is an integral part of the Makeup and Purification System. HPI is automatically actuated (backed-up by manual actuation) by the ESAS upon detection of either a low coolant system pressure ($\leq$1500 psig) or high reactor building pressure ($\geq$4 psig). A safety injection signal switches the Makeup System from its normal operating mode to the emergency (HPI) mode. In the emergency mode, borated water is injected into the reactor vessel, with the HPI pumps taking suction from the Borated Water Storage Tank (BWST).


FROM
INDUSTRIAL
COOLERS
FROM
NSCCCS
P
SWV-
162
SWV
366
P
SWV
363
FE
SWV 36
SWV-35
FE
P
SWV-38
SWV-37
FE
P
SWV 106
SWV-39
TO
INDUSTRIAL
COOLERS
TO
NSCCCS
P
SWV
161
P
SWV-
364
P
SWV
365
RBECS
FE
P
SWV 308
SWV 46
FE
P
SWV 44
SWV 43
FE
P
SWV 42
SWV-41
REACTOR
BUILDING
REACTOR BUILDING SPRAYS
CORE
FLOODING
TANK
CORE
FLOODING
TANK
N.O.
CFV-6
CFV-4
DHV-1
SH
CFV-3
CFV-1
SH
CFV-5
RCP-1A
RCP-1B
MUV-43
MUV 42
SH
REACTOR
VESSEL
MUV-38
SH

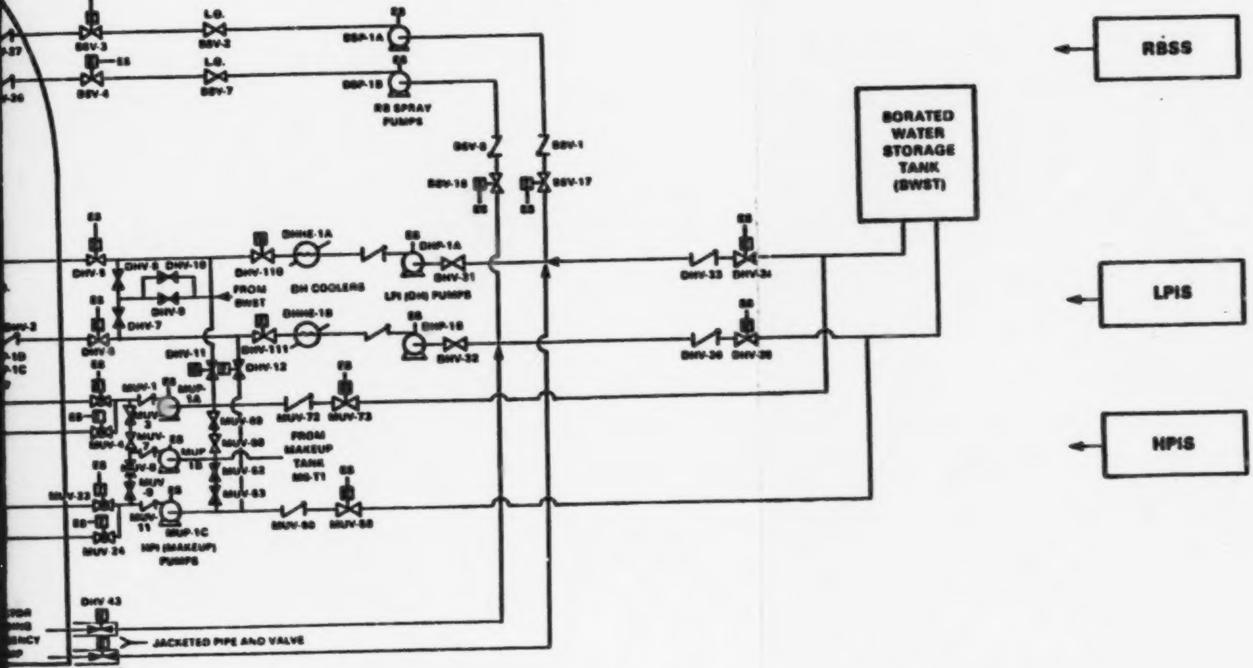

ES
BSV-3
L.O.
BSV-2
ES
BSP-1A
ES
BSV-4
L.O.
BSV-7
BSP-1B
RB SPRAY PUMPS
BSV-8
BSV-1
BSV-16
BSV-17
ES
DHV-5
DHV-8
DHV-10
DHV-9
DHV-7
DHV-6
FROM BWST
DHV-110
DHHE-1A
DH COOLERS
DHHE-1B
DHV-111
DHP-1A
DHV-31
LPI (DH) PUMPS
DHP-1B
DHV-32
DHV-11
DHV-12
DHV-33
DHV-34
DHV-36
DHV-35
MUV-1
MUP-1A
MUV-3
MUV-4
MUV-7
MUP-1B
MUV-9
MUV-11
MUP-1C
HPI (MAKEUP) PUMPS
MUV-23
MUV-24
MUV-69
MUV-68
MUV-62
MUV-63
MUV-72
MUV-73
FROM MAKEUP TANK MU-T1
MUV-80
MUV-58
DHV 43
DHV 42
JACKETED PIPE AND VALVE
BORATED WATER STORAGE TANK (BWST)
RBSS
LPIS
HPIS

FIGURE 3.4

SIMPLIFIED SCHEMATIC DIAGRAM OF ENGINEERED SAFEGUARDS SYSTEM FOR CORE AND BUILDING PROTECTION

The HPI system can be used also for the so-called "feed and bleed" operation. The feed and bleed operation, manually initiated and controlled, removes heat from the primary coolant if secondary heat removal capability is lost (i.e., loss of all main and emergency feedwater). System pressure is reduced (energy removed) by blowing down reactor coolant through the pressurizer power operated relief valve (PORV) and injection of cold water by HPI.

Core Flood Tank (CFT)-System

The CFT-system is designed to provide core protection continuity for intermediate and large size LOCAs. It consists of two independent water tanks, whose contents are pressurized to about 600 psig by nitrogen. Two check valves in each discharge line prevent reactor coolant from entering the CFTs when the RCS pressure is higher than the tank pressure. The same check valves open and admit the content of the CFTs into the RCS if the RCS pressure falls below that of the CFTs. Thus, the CFT-system is a passive system requiring no control or operator action to actuate. Each discharge line is connected to a Low Pressure System injection line, sharing one of the two check valves with the LP system.

Low Pressure Injection (LPI)

The low pressure system operating in the injection mode (LPI) is designed to maintain core cooling for break sizes ranging from intermediate breaks to the doubled ended rupture of the largest pipe. The system is used during normal shutdown operations to remove shutdown decay heat from the RCS by taking suction from one hot leg, pumping the water through a heat exchanger and returning it to the reactor vessel. The system is called the Decay Heat Removal System in this normal shutdown mode.

The LPI system consists of two redundant trains. The LPI pumps take suction from the BWST, pass the borated water through a heat exchanger, and discharge directly into the reactor vessel through core flooding nozzles on opposite sides of the vessel. The core flooding nozzles are shared with the CFT-system. The LPI system is provided with a crossover line to permit one train flow of 3,000 gpm to be split between both core flood nozzles should one LPI pump fail.

The LPI system is actuated by the ESAS. The LPI pumps receive a start signal when the RCS-pressure is less than 1500 psig and the closed injection valves are opened when the RCS pressure falls below 500 psig. The system is also automatically actuated when the reactor building pressure rises above 4 psig.

ECCS Recirculation Mode

When the BWST reaches a low water level, an alarm will be annunciated in the control room. At this time the operator must switch to the recirculation mode, i.e., recirculate reactor coolant and injection water collected in the containment sump. The operator is required to open the suction valves in the recirculation line from the sump. If the HP-system is required to operate in the recirculation mode, the LP- and the HP-system must be aligned so that the LP-system supplies the suction side of the HP-pumps. This requirement for a "boosted" supply for the HP-pumps exists because the water level in the sump does not provide sufficient suction head to these pumps.

3.4.2 Reactor Building Cooling and Spray Systems

The Reactor Building Emergency Cooling System (RBECS)[1] and the Reactor Building Spray System (RBSS) are independent and redundant systems. They are designed to limit the post-accident pressure in the containment to less than the design value and to reduce the pressure to nearly atmospheric pressure.

The RBECS consists of three fan coolers whose heat exchangers are served by the Nuclear Services Closed Cycle Cooling System. The RBSS consists of two pump trains and injects water into the containment through two spray headers. The RBSS shares the suction line header from the BWST and from the sump with the LP-system. The RBSS also serves as an iodine (fission product) removal system in addition to its role in reducing pressure. The RBECS is actuated by the ESAS (via RBIC, see Section 3.3) when the containment pressure rises above 4 psig; the RBSS is actuated when the containment pressure rises above 30 psig.

---

[1] The RBECS is the emergency operating mode of the Reactor Building Cooling System (RBCS).

Combinations of RBECS and RBSS equipment required to reduce the post-accident containment pressure are defined in Section 4.

3.5 EMERGENCY FEEDWATER SYSTEM (EFS)

The purpose of the Emergency Feedwater System (EFS) is to remove post-shutdown decay heat from the coolant system via the steam generators if the power conversion system (the normal heat removal system) is not available.

The EFS is an interconnected two-train system, each train capable of supplying emergency feedwater to either or both steam generators under automatic or manual initiation and control. The primary water source is the Condensate Storage Tank. An alternate source of water is available from the main condenser hotwell. The Train A pump of the EFS is turbine-driven, with motive steam supplied from either steam generator.

The Train B pump is motor-driven and powered from a diesel-backed engineered safeguards bus. At the present time, both pumps are cooled by the NSCCCS, creating an undesirable dependency on AC-power. However, the Florida Power Corporation has made a commitment to eliminate this dependency by making both pumps self-cooled (3-2). This study assumes self-cooled EFS pumps.

The turbine-driven train is independent of any other auxiliary system except for the steam admission valve, which is powered from DC-power bus B.

3.6 EMERGENCY AUXILIARY SYSTEMS

The engineered safeguard systems are dependent on electric power to operate pumps and valves and on cooling systems which provide cooling to pumps and motors. The following subsections briefly describe the individual emergency auxiliary systems.

3.6.1 Electric Power

The Unit 3 start-up transformer serves as the normal source for engineered safeguards auxiliaries. Power to this transformer is provided from any one of five 230 kV transmission circuits (tne normal offsite power source) or from any one of the existing on-site fossil Units 1 and 2. Both Units 1 and 2 are designed to continue in operation following load rejection from 100 percent load down to unit auxiliary load without a turbine trip. The credit taken for Units 1 and 2 in this analysis is discussed in Appendix D.

Upon loss of offsite power, power is supplied from two automatic, fast-start-up diesel engine generator units. These are sized so that either one can carry the required engineered safeguards load. Each emergency generator unit feeds one engineered safeguards 4160 volt bus (Bus 3A or 3B). Each generator is capable of continuously supplying the entire connected safeguards load plus selected balance-of-plant emergency loads on one 4160 volt bus.

3.6.2 Emergency Cooling Systems

Cooling of the engineered safeguard pumps and motors (and the RBECS fans) is supplied by two independent systems, the Nuclear Services Cooling Water System (NSCWS) and the Decay Heat Services Cooling Water System (DHCWS). A schematic of both systems is shown in Figure 3.5.

Nuclear Services Cooling Water System

The NSCWS is comprised of the single loop Nuclear Services Closed Cycle Cooling System (NSCCCS) and the once-through Nuclear Services Seawater System (NSSWS). During emergency operation, the NSCCS provides a heat sink for equipment essential to the safety of the plant and provides a redundant function to the RBSS by removing heat from the containment via the RBECS. It also provides an intermediate loop between the primary coolant and the seawater.

The NSCCCS consists of one normally operating pump (SWP-1C), which is not rated for emergency flow, and two 100% rated emergency pumps. Each emergency pump (SWP-1A and 1B) consists of two half-sized pumps driven by a single shaft.

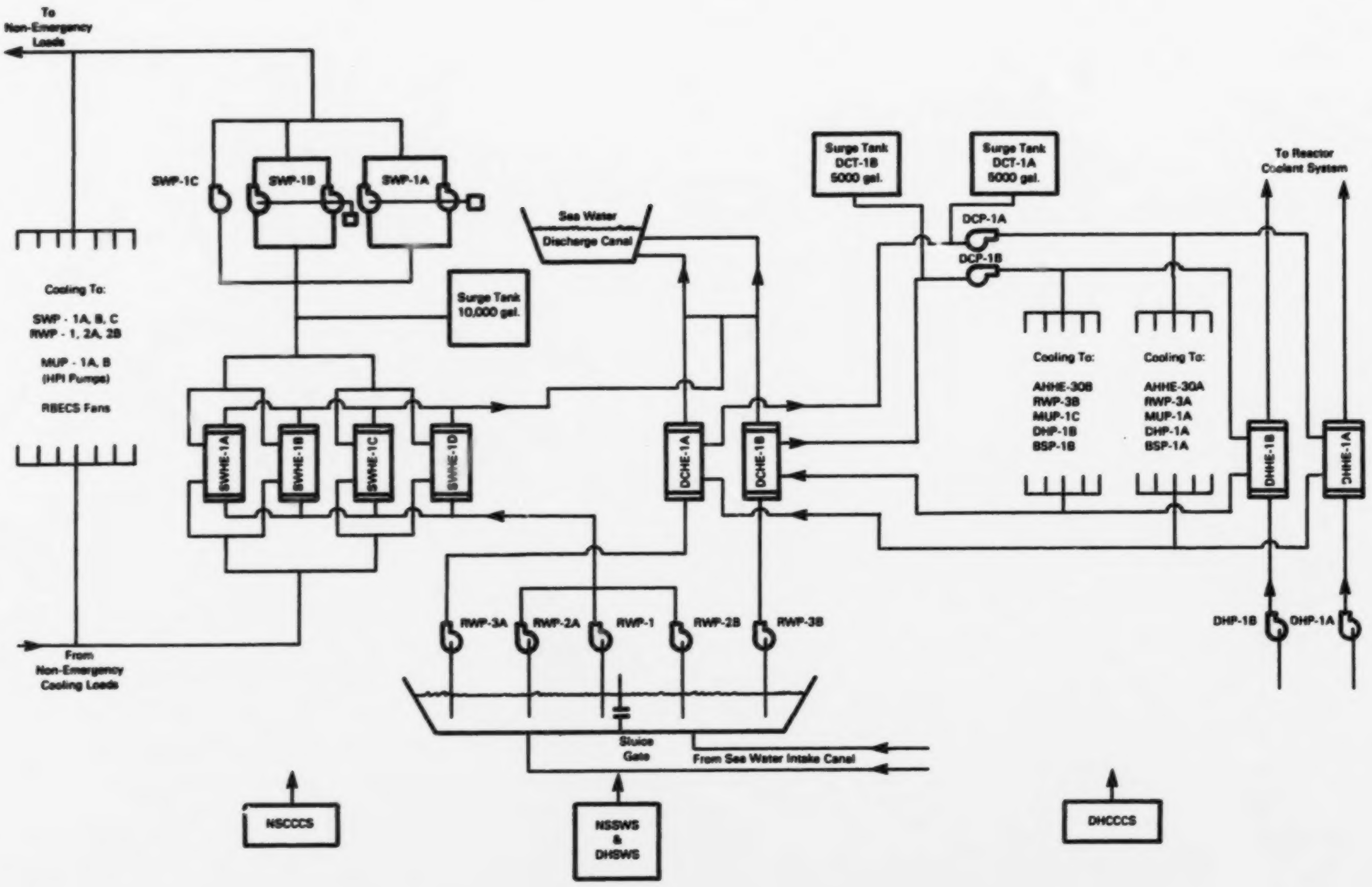

To Non-Emergency Loads
Cooling To:
SWP - 1A, B, C
RWP - 1, 2A, 2B
MUP - 1A, B
(HPI Pumps)
RBECS Fans
From Non-Emergency Cooling Loads
SWP-1C
SWP-1B
SWP-1A
Surge Tank 10,000 gal.
SWHE-1A
SWHE-1B
SWHE-1C
SWHE-1D
Sea Water Discharge Canal
DCHE-1A
DCHE-1B
Surge Tank DCT-1B 5000 gal.
Surge Tank DCT-1A 5000 gal.
DCP-1A
DCP-1B
To Reactor Coolant System
Cooling To:
AHHE-30B
RWP-3B
MUP-1C
DHP-1B
BSP-1B
Cooling To:
AHHE-30A
RWP-3A
MUP-1A
DHP-1A
BSP-1A
DHHE-1B
DHHE-1A
DHP-1B
DHP-1A
RWP-3A
RWP-2A
RWP-1
RWP-2B
RWP-3B
Sluice Gate
From Sea Water Intake Canal
NSCCCS
NSSWS & DHSWS
DHCCCS

FIGURE 3.5. SIMPLIFIED SCHEMATIC DIAGRAM OF THE EMERGENCY COOLING (NSCCCS, DHCCCS) SYSTEMS: NO VALVES SHOWN

The NSSWS has one normally operating pump (RWP-1), which is not rated for emergency flow, and two 100% rated emergency pumps (RWP-2A,B).

The heat absorbed by the NSCCCS is transferred to the NSSWS by a bank of four one-third capacity heat exchangers. Three operable heat exchangers are required for both emergency and normal operation.

Decay Heat Services Cooling Water System

The DHCWS is comprised of the two loop Decay Heat Closed Cycle Cooling System (DHCCCS) and the once-through Decay Heat Seawater System (DHSWS). The DHCCCS provides an intermediate loop between the primary coolant and the seawater. During emergency operation, the DHCCCS removes decay heat from the LP-heat removal system and it provides a heat sink for pumps and motors in the LP-system, the RBSS and one train of the HP-system (MUP-1C). Operation is also required during normal shutdown to remove reactor shutdown decay heat.

The DHCCCS consists of two completely independent 100% capacity trains. Because there are no cross-ties between the two trains, each train only cools equipment in the respective train of the system served.

The DHSWS is an open once-through two-train system, transporting heat from the DHCCCS to the seawater discharge canal. Each DHSWS-train is rated at 100% capacity and services only its respective DHCCCS-train.

3.7 CONNECTIONS BETWEEN CR-3 AND COAL-FIRED UNITS 1 AND 2

Two safety-related connections which exist between the nuclear and coal-fired units are noteworthy. The first is a hot steam line from CR-1 and CR-2 which is connected to CR-3 through a normally-closed manually operated valve at a point immediately upstream of the steam admission valve to the CR-3 turbine-driven emergency feedwater pump. The second is an AC-power connection through the startup transformer for CR-1 and CR-2 which can supply emergency AC power to the 4.16 KV engineered safeguard (ES) busses in CR-3. This means of supply to the 4.16 KV (ES) busses is an alternate manual backup in the event of loss-of-offsite power, shutdown of CR-3 and failure of the emergency diesel generators. Both of these connections are described and evaluated in the relevant appendices to this report.

References

3-1 Florida Power Corporation, "Crystal River Unit 3 Nuclear Generating Plant Final Safety Analysis Report," Docket 50-302, 1971 (as amended through March 26, 1976).

3-2 Letter from Ronald M. Bright, Florida Power Corporation to Frank Rowsome, NRC, Subject: Utility Review of SAI Report "Brief Results to Date Crystal River-3 Safety Study", April 29, 1980.

4.0 EVENT TREES

This chapter identifies the categories of initiating events considered and describes the event trees constructed to delineate the accident sequences that stem from each initiator. Analyses are also presented for three special events which are shown to have very small probabilities and for which no detailed event trees are developed. Discussion of the quantitative evaluation of those sequences delineated by event trees is deferred to the next chapter.

4.1 Initiating Events

The basic set of initiating events considered as potential accident initiators for CR-3 are:

1. Transients
2. Loss of Coolant Accidents (LOCA)
3. Interfacing Systems LOCA
4. Vessel Rupture
5. Steam Generator Tube Rupture

These initiators, which are the same as those considered in the Reactor Safety Study (4-1), may generally be considered as originating within, or "internal" to, the plant. Initiating events originating outside the plant, such as earthquake, flooding, aircraft impact, or other similar "external" events, and sabotage are outside the scope of the project and are not addressed.

Each of the five "internal" initiating event types listed above was carefully examined for applicability and relative probability prior to the development of event trees for the plant. This effort resulted in identification of only two of these, transients and LOCAs, as requiring the development and construction of detailed event trees. Analyses of the remaining three events are presented in Section 4.4.

4.1.1 Transient Initiators

A transient event is defined as any abnormal condition in the plant which requires that the plant be shutdown, but which does not directly breach reactor coolant system (RCS) integrity. Many event types fall into this category. Reference 4-2 (EPRI NP-801), which was used as the basis for transient event data in the present analysis, is the most current and complete listing of such event types available. It tabulates and provides data for 41 different PWR transient types. A careful review of this information resulted in the determination that these transients could be broken down into two basic types:

- Type T_1

  Transients which leave the Power Conversion System (PCS) capable of operation, i.e., it is possible to continue normal secondary heat removal.

- Type T_2

  Transients which directly cause the operation of the PCS to be interrupted, such as loss of main feedwater, condenser isolation, loss of offsite power, etc.

A more detailed review and evaluation of the two transient types identified one particular transient in each major type that could not be described only in terms of its effect on the PCS because it affected other mitigating systems. These two transients were loss of component cooling within Type 1 and loss of offsite power within Type 2. These were separated out and designated subtypes T_{1A} and T_{2A}, respectively. The resulting four transient categories are used in the subsequent analysis and evaluation. The frequencies for each of these four categories, obtained from EPRI NP-801, are shown in Table 4.1

Table 4.1 Transient Event Frequencies[1]

		Events/Year
Transients with PCS Available		
T_{1A}	: Loss of NSCCCS	0.01
T_1-T_{1A}	: All other T_1 Transients	8.48
T_1	: All T_1 Transients	8.49
Transients with PCS Not Available		
T_{2A}	: Loss of Offsite Power	0.32
T_2-T_{2A}	: All other T_2 Transients	1.78
T_2	: All T_2 Transients	2.10
All Transients		10.59

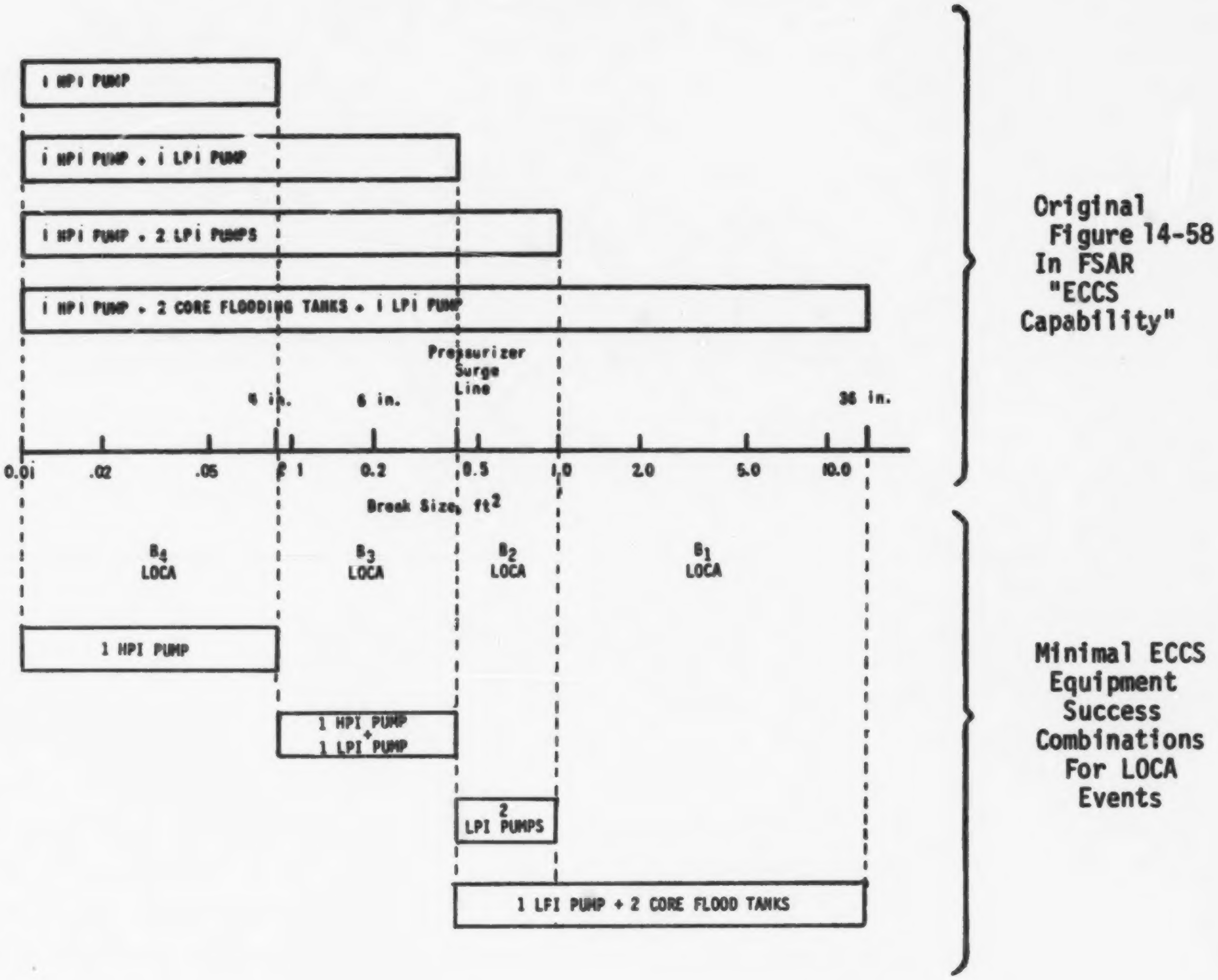
[1] Data from Reference 4-2 (EPRI NP-801)

4.1.2 LOCA Initiators

A LOCA is defined as a breach of the pressure boundary of the RCS which causes an uncontrollable loss of water. Various categories of LOCA events can be defined in terms of the minimum sets of equipment capable of successfully responding to each. These differ from plant to plant. Four LOCA categories were defined for CR-3 as a result of an examination of the Final Safety Analysis Report (4-3). These four LOCAs are referred to as large (B_1), medium (B_2), small (B_3), and small-small (B_4), and they represent flow areas of greater than 1 square foot, between 1 square foot and 0.4 square feet, between 0.4 square feet and 0.087 square feet, and less than 0.087 square feet, respectively. The basis of these break categories is shown in Figure 4.1. The upper half of the figure, taken from the Final Safety Analysis Report (FSAR), shows four different equipment success combinations and the break size ranges they cover. These equipment combinations, however, are not minimal. For example, the combination of one HPI pump and one LPI pump is shown as successful from 0 - 8.5 inches; but one HPI pump alone is also shown as successful from 0-4 inches. Therefore, one LPI pump is not required from 0-4 inches and the combination of one HPI pump and one LPI pump is not minimal over that range. Similar considerations resulted in the development of the lower half of the figure to identify and define unique minimal equipment combinations for the four specific LOCA size ranges shown. Note that the requirement for one HPI pump was removed for the B_1 and B_2 LOCAs. This is based on the LOCA blowdown curves in the FSAR, which indicate that RCS pressure drops quickly enough for these break sizes to not require injection from the HPI pump. The initiating event frequency for each of the four LOCA categories is shown in Table 4.2. The basis for these frequencies is later described in detail in Section 5.3.2.

4.2 Transient Event Tree

A single event tree was designed and constructed to represent plant response to both of the two basic transient types described above. This is feasible because plant response to any transient, regardless of type, requires the same plant functions to be performed. The transient type, however, does specify the conditions under which those functions must be performed. The event tree constructed, shown in Figure 4.2, includes all the functions required to bring the plant to a hot shutdown condition as well as the consequence mitigating functions considered in scenarios where core damage occurs. The functions include reactor shutdown (Subcriticality), removing the heat from the RCS (Normal and Emergency Secondary Heat Removal), RCS overpressure protection (Primary System Pressure Relief Requirement and Primary System Pressure Relief), preventing the transient from becoming a LOCA (Primary System Integrity), direct cooling of the primary by injecting


1 HPI PUMP
1 HPI PUMP + 1 LPI PUMP
1 HPI PUMP + 2 LPI PUMPS
1 HPI PUMP + 2 CORE FLOODING TANKS + 1 LPI PUMP
Pressurizer Surge Line
4 in.
6 in.
36 in.
0.01
.02
.05
0.1
0.2
0.5
1.0
2.0
5.0
10.0
Break Size, ft²
B4 LOCA
B3 LOCA
B2 LOCA
B1 LOCA
1 HPI PUMP
1 HPI PUMP + 1 LPI PUMP
2 LPI PUMPS
1 LPI PUMP + 2 CORE FLOOD TANKS
Original Figure 14-58 In FSAR "ECCS Capability"
Minimal ECCS Equipment Success Combinations For LOCA Events

LEGEND:

HPI - HIGH PRESSURE INJECTION
LPI - LOW PRESSURE INJECTION

Figure 4.1 Minimal Emergency Coolant Injection Equipment Success Combinations for LOCA Events at CR-3 (Reference 4-3)

Table 4.2 LOCA Frequencies[1]

Initiator	Definition	Events/Year
B_1	Large LOCA - a breach of the RCS with a flow area greater than 1 ft^2 (B_1>13.5" diameter)	1.0 E-4
B_2	Medium LOCA - a breach of the RCS with a flow area greater than 0.4 ft^2 and less than or equal to 1 ft^2 (13.5"≥B_2>8.5" diameter)	1.0 E-4
B_3	Small LOCA - a breach of the RCS with a flow area greater than 0.087ft^2 and less than or equal to 0.4 ft^2 (8.5"≥B_3≥4" diameter)	1.0 E-4
B_4	Small-Small LOCA - a breach of the RCS with a flow area less than or equal to 0.087 ft^2 (4"≥B_4 diameter)	1.3 E-3

---

[1] Based on data in WASH-1400, Appendix III (Ref. 4-4)

BEST DOCUMENT AVAILABLE

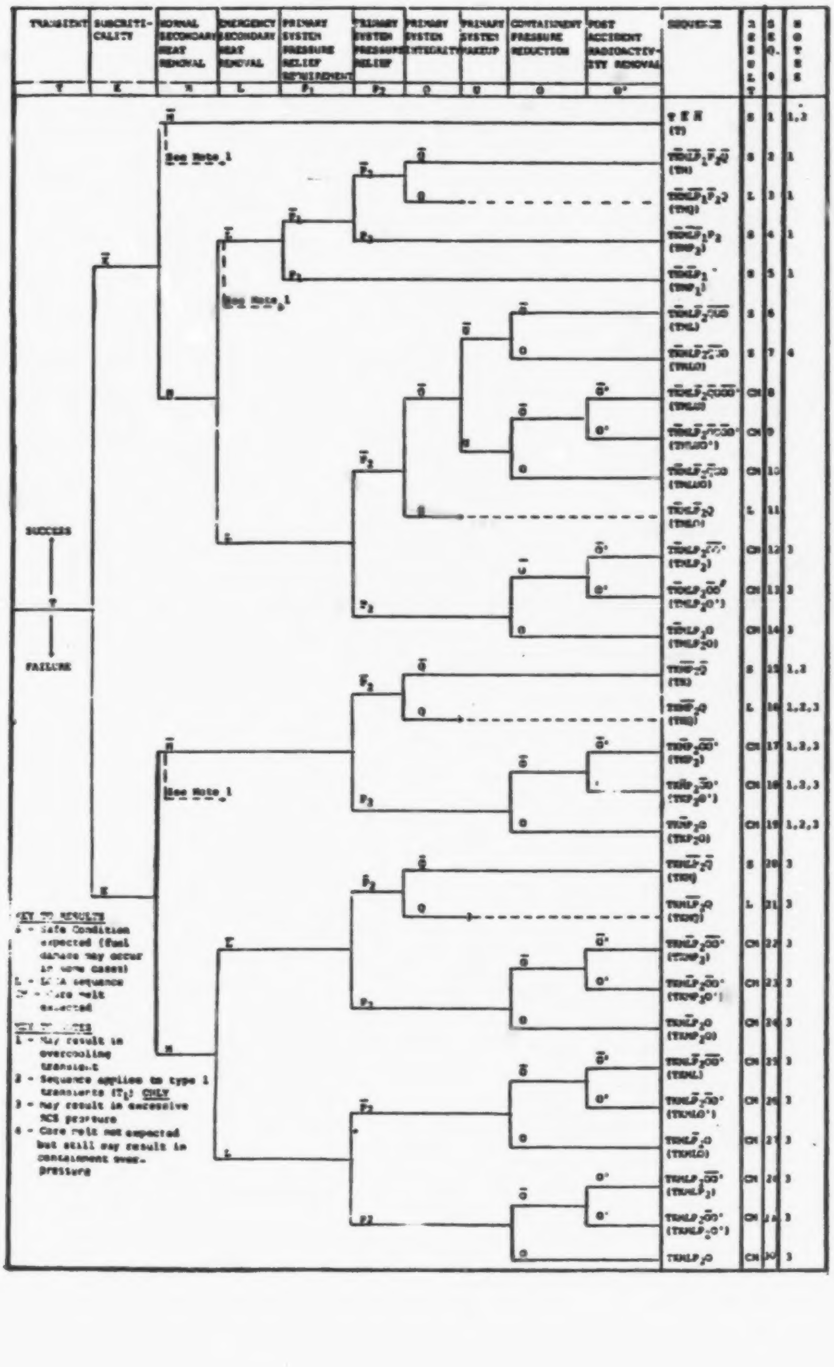

TRANSIENT
T
SUBCRITI-CALITY
K
NORMAL SECONDARY HEAT REMOVAL
M
EMERGENCY SECONDARY HEAT REMOVAL
L
PRIMARY SYSTEM PRESSURE RELIEF REQUIREMENT
P1
PRIMARY SYSTEM PRESSURE RELIEF
P2
PRIMARY SYSTEM INTEGRITY
Q
PRIMARY SYSTEM MAKEUP
U
CONTAINMENT PRESSURE REDUCTION
O
POST ACCIDENT RADIOACTIVITY REMOVAL
O'
SEQUENCE
RESULT
SEQ. #
NOTES
See Note 1
SUCCESS
FAILURE
KEY TO RESULTS
S - Safe Condition expected (fuel damage may occur in some cases)
L - LOCA sequence
CM - Core melt expected
KEY TO NOTES
1 - May result in overcooling transient
2 - Sequence applies to type 1 transients (T1) ONLY
3 - May result in excessive RCS pressure
4 - Core melt not expected but still may result in containment over-pressure

Figure 4.2 Transient Event Tree for Crystal River-3

coolant (Primary System Makeup), and consequence reduction by preventing containment overpressure (Containment Pressure Reduction) and removing radioactivity from the containment atmosphere (Post-Accident Radioactivity Removal).

The second and fourth columns from the right accompanying the event tree (Figure 4.2) provide information useful in shorthand designations of the sequences. The column headed SEQUENCE represents the sequences in the style used in the Reactor Safety Study, with appropriate symbols representing the event tree branches and a bar over the symbol to denote success rather than failure. The shorter designations appearing in parentheses simply omit the successes. The initial T indicates the transient initiator; a subscript would indicate a specific type of transient. Throughout this report, a simpler designation is used at some expense to the descriptive content. The sequences are numbered consecutively in the column headed SEQ #. The appropriate sequence number is used as a subscript to the symbol T to identify a particular generic sequence from the transient event tree. A specific sequence is represented by appending the generic sequence representation to the appropriate initiator symbol, for example T_{2A} T_{10} and $(T_1 - T_{1A})$ T_8.

The RESULT column indicates the outcome of the sequences in terms of the fate of the reactor core, with the key appearing in the figure itself. The NOTES column refers to notes which also appear in the figure.

Some adjustments are necessary to accommodate the use of a single generic event tree for several types of initiators. For example, type T_1 transients imply the event $\overline{M}$, hence the event M is excluded by definition. The type T_1 sequences containing M (T_2 through T_{14} and T_{20} through T_{30} in this case) may be assigned zero probabilities or they may be omitted from tabulations of sequence probabilities. The same is true of type T_2 transient sequences containing $\overline{M}$.

The two basic transient types discussed earlier have an effect on the reliability of various plant functions required to be performed in response to a transient. These transient types, however, affect only the reliability of the function--not the need for it. For example, all loss of PCS transients (type T_2) have a direct effect on the availability of the primary heat removal functions, since the PCS itself is no longer available to perform that function. Loss of offsite power transients (type T_{2A}) have an additional direct effect on all functions which require electric power.

Transients which do not result in loss of PCS (type T_1) do not affect function reliabilities, but the type T_{1A} subset (loss of NSCCCS) causes the RBCS to become unavailable to perform the containment heat removal function. The type T_{1A} transient also causes one train of HPI to become unavailable for the primary heat removal function.

All of the functions included in the event tree, and their failure criteria are described in Table 4.3. The event tree was constructed by considering the timing sequence of the accident as well as the following functionability/operability interrelationships between events (functions and/or systems):

1. If Normal Secondary Heat Removal succeeds (event $\overline{M}$), then Emergency Secondary Heat Removal doesn't matter since both functions provide water to the secondary side of steam generators in order to remove heat from the RCS. Thus, only one of these functions is required for any given sequence.

2. If Subcriticality and Normal Secondary Heat Removal succeed (events $\overline{K}$ and $\overline{M}$), then Primary System Pressure Relief, Primary System Integrity, and Primary System Makeup don't matter. The justification for this is that the pressure in the RCS would not reach the relief pressure, thus pressure control is not required, and since no RCS inventory would be lost, no makeup is required.

3. If Primary System Pressure Relief fails (event P_2), Primary System Integrity and Primary System Makeup don't matter, and core melt is assumed. This highly conservative assumption is justified because the very small probability of event P_2 (failure of S/RVs to open when demanded) is expected to cause all accident sequences containing that event to be relatively small contributors to risk. (Exception: Core melt is not assumed if event P_2 occurs in the sequence where subcriticality and Emergency Secondary Heat Removal succeed, Normal Secondary Heat Removal Fails, and Primary System Pressure Relief is required (events $\overline{K}M\overline{L}\overline{P}_1$) because the excess RCS pressure is not expected to be very great).

4. If Primary System Integrity fails (event Q) the sequence results in a LOCA, and the sequence (and analysis) is continued in a LOCA event tree. This is justified by the fact that the rate of leakage of RCS inventory is sufficient to fit the definition of a LOCA.

BEST DOCUMENT AVAILABLE

Table 4.3 Event Definitions for Transient Event Tree

T	Transient - Any abnormal condition in the plant which requires that the plant be shut down, but does not directly breach RCS integrity. • Type 1 Transient (T_1) - a transient which does not directly affect the operability of the PCS (Normal Secondary Heat Removal). • Type 2 Transient (T_2) - a transient which directly affects the operability of the PCS, causing it to become inoperative.[1]
K	Subcriticality - Failure of automatic (or manual) reactor scram by some time t_0.
M	Normal Secondary Heat Removal - Failure of the PCS to remain in uninterrupted operation following a transient, providing sufficient main feedwater (MFW) flow to the steam generators to remove primary heat for 24 hours. • For sequences with event $\bar{K}$, sufficient is defined as 6% of maximum MFW flow. • For sequences with event K, sufficient is defined as 100% of maximum MFW flow initially, and sufficient flow for the equilibrated power level for the remainder of the 24 hours (this level depends on the specific transient).
L	Emergency Secondary Heat Removal - Failure to provide sufficient feedwater flow (defined as 6% of maximum MFW flow) to the steam generators by some time t_1 and maintain it for 24 hours, by one of the following methods: • For sequences with event $\bar{K}$: 1. Automatic activation of emergency feedwater system (EFS) 2. Manual actuation of EFS (if automatic fails) 3. Manual recovery of PCS • For sequences with event K: 1. Automatic activation of EFS
P_1	Primary System Pressure Relief Requirement - Failure to require the RCS pressure relief function (i.e. - RCS pressure does not exceed relief setpoint).
P_2	Primary System Pressure Relief - Failure of sufficient S/RVs to open and relieve excess primary system pressure, given the requirement.
Q	Primary System Integrity - Failure of any S/RVs which opened to reseat.
U	Primary System Makeup - Failure to establish flow from BWST to the RCS using at least one charging pump (for the purpose of a "bleed and feed" operation).
O	Containment Pressure Reduction - Failure to remove heat from the containment atmosphere by the use of at least one Reactor Building Fan or at least one Reactor Building Spray Subsystem.
O'	Post Accident Radioactivity Removal - Failure to remove radioactive effluents from the containment atmosphere by the use of at least one Reactor Building Spray Subsystem.

---

[1] Type 2 transients do not apply to Sequences 1 and 15-19 in Figure 4.2 since the PCS remains operable in those sequences.

5. Containment Pressure Reduction and Post-Accident Radioactivity Removal functions are considered only in those sequences which result in core melt since these functions serve only to reduce the consequences of core melt accidents, and they would not serve any purpose in other transient situations. (Exception: Containment Pressure Reduction is considered in the situation where Subcriticality succeeds (event $\overline{K}$), all Secondary Heat Removal fails (events M,L), and Primary System Pressure Relief, Integrity, and Make-up succeed (events $\overline{P}_2$, $\overline{Q}$, and $\overline{U}$. In this particular case, which is called a "feed and bleed" operation, core melt is prevented by removing decay heat through the S/RVs and replacing the coolant with the makeup system. However, this will cause a buildup of steam in the containment, which may necessitate use of Containment Pressure Reduction to prevent containment overpressure).

6. If Containment Pressure Reduction fails (event O), the Post-Accident Radioactivity Removal (PARR) is assumed to fail based on the failure criteria for these events. If the failure criteria is met for Containment Pressure Reduction, then it must also be met for PARR (see Event Definitions in Table 4.3).

These interrelationships reduce the number of possible sequences from 512 to 30.

Some differences from the event tree developments in the Reactor Safety Study may be of particular interest. In this study, emergency electric power was treated only at the fault tree level, as were other support systems, rather than as a functional heading on the event tree. This is adequate and does not change the substance of the analysis in any essential way. In addition, the sodium hydroxide addition (SHA) system was not included in the CR-3 analysis, since it was found in the Reactor Safety Study itself that the enhancement of radioactivity removal by the sprays due to SHA is not significant. CR-3 also has a sodium thio-sulphate addition system (which at the time of this analysis was disabled by locked-closed valves); this system was also not included in the analysis.

For this study, systems required for long-term cooling to cold shutdown after a transient were not included on the transient tree. These systems do not affect the occurrence of core melt or the radioactive release. It was assumed that being in a stable hot shutdown condition was sufficient. These systems were included in the Reactor Safety Study.

On the other hand, the Reactor Safety Study transient event tree did not include the containment overpressure protection or post-accident radioactivity removal functions. In this study, these systems were included for all transient core mèlt sequences, since they can affect the containment failure mode and release categories of the sequence.

The equipment success requirements related to the functions defined in Table 4.3 are indicated in Table 4.4 . These form the basis for "top event" definitions used for system fault tree analysis as discussed later in Chapter 5.

Table 4.4 Definition of Equipment Success Requirements for Transient Events in Crystal River-3

TRANSIENT TYPE	SUBCRITICALITY	NORMAL SECONDARY HEAT REMOVAL	EMERGENCY SECONDARY HEAT REMOVAL	PRIMARY SYSTEM PRESSURE RELIEF REQUIREMENT	PRIMARY SYSTEM PRESSURE RELIEF	PRIMARY SYSTEM INTEGRITY	PRIMARY SYSTEM MAKEUP	CONTAINMENT PRESSURE REDUCTION	POST ACCIDENT RADIOACT REMOVAL
OPERATION OF POWER CONVERSION SYSTEM NOT AFFECTED (T_1)	AUTOMATIC OR MANUAL REACTOR SCRAM OCCURS	PCS REMAINS IN UNINTERRUPTED OPERATION AT 6% OF FULL POWER FLOW (FPF)	AUTOMATIC OR MANUAL ACTUATION OF EMERG. FW SYSTEM OR RECOVERY OF PCS (6% FPF)	RCS PRESSURE EXCEEDS RELIEF SETPOINTS	1/3 S/RVS OPENS	ALL S/RVS RESEAT	1/3 MAKEUP PUMPS ALIGNED TO BWST	1/3 FAN COOLERS OR 1/2 SPRAY SUBSYSTEM W/RECIRC.	1/2 SPRAY SUBSYSTEM W/RECIRC.
OPERATION OF POWER CONVERSION SYSTEM AFFECTED (FAILED) (T_2)	↓	FAILS	↓	↓	↓	↓	↓	↓	↓

There are eight non-melt sequences on the event tree, indicated on Figure 4.2 by the "S" in the Result column. For sequences 1,2,4, and 5, core melt is prevented by success of Subcriticality (shutting down the nuclear reaction), removal of the decay heat by either Normal or Emergency Secondary Heat Removal, and maintaining RCS integrity by either not lifting the S/RVs, or by having them reseat if they do lift.[1] For sequences 6 and 7, core melt is prevented by establishing a "feed and bleed" operation, as earlier described in the exception to functionability/operability interrelationship number 5. For sequences 15 and 20 (ATWS sequences), core melt is prevented by (1) providing heat removal from the primary by success of Normal or Emergency Secondary Heat Removal, and (2) handling the initial pressure spike (caused by failure of Subcriticality) by Primary System Pressure Relief (lifting the S/RVs). In this situation, reactor power will stabilize at a power level equivalent to the percentage of full main feedwater flow being provided to the steam generator(s). This power level can be maintained until negative reactivity can be added to shutdown the reactor.

There are four sequences on the tree, indicated in Figure 4.2 by the "L" in the Result Column, which lead to LOCAs. These sequences are continued in a LOCA event tree and are handled as special cases of LOCA sequences. In contrast, the Reactor Safety Study included transient-induced LOCAs directly on the transient event tree and automatically assumed they led to core melt.

4.3 LOCA Event Tree

A single event tree was constructed to represent plant response to all four of the LOCA categories described in the previous section. A single tree is considered adequate because plant response to any size LOCA requires the same basic plant functions to be performed. The particular break size, however, specifies the conditions under which those functions must be performed. The event tree constructed, shown in Figure 4.3, includes all systems/functions required to keep the core from melting and to minimize radiation release to the environment. The systems/functions include reactor shutdown (Reactor Subcriticality), keeping the core cooled during the injection phase of the LOCA (Emergency Coolant Injection), preventing containment overpressure during injection (Reactor Building Spray Injection and Reactor

---

[1] It is important to note that these sequences (and sequences 3 and 15-19) have the potential for causing an overcooling transient by providing too much Secondary Heat Removal.

BEST DOCUMENT AVAILABLE

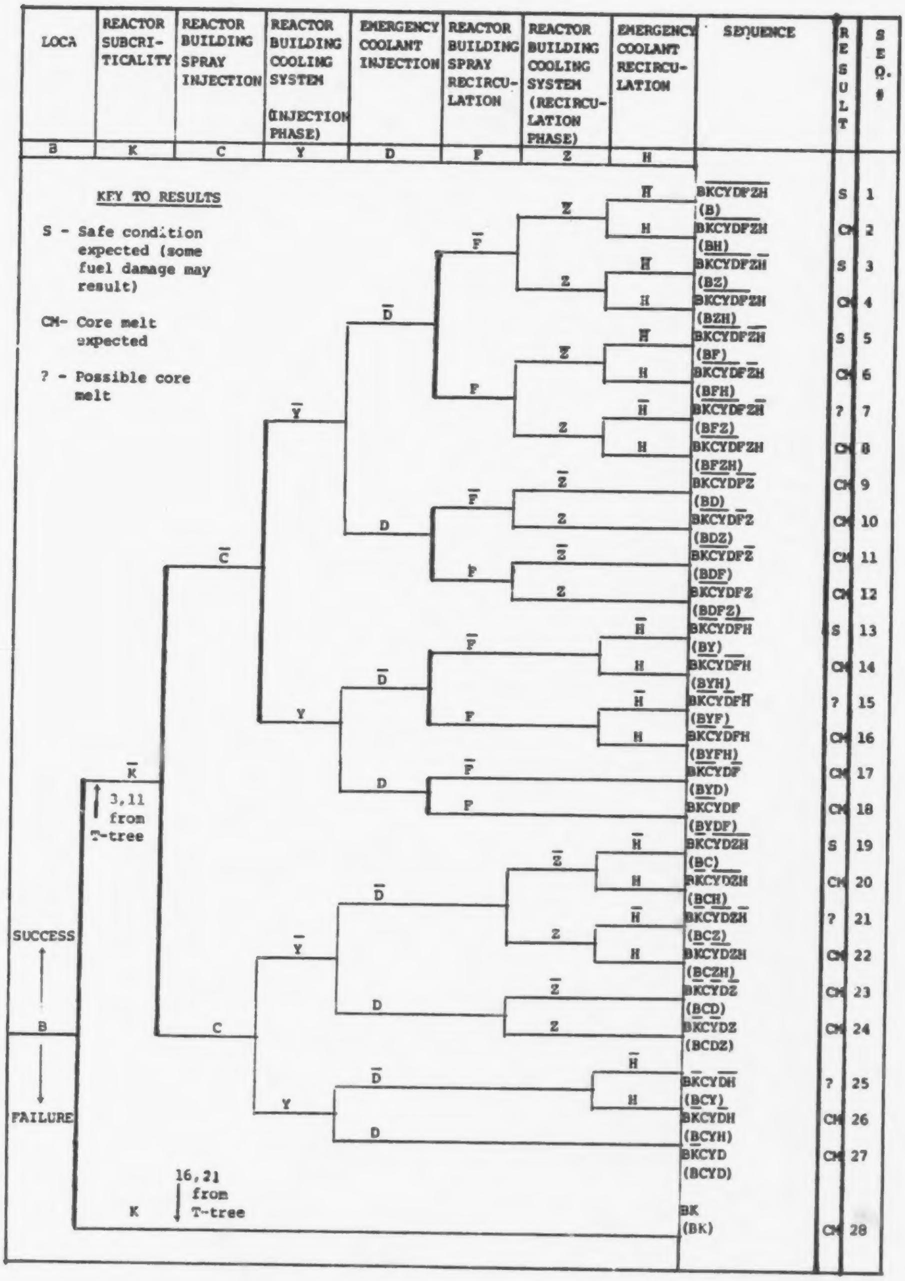

LOCA
REACTOR SUBCRITICALITY
REACTOR BUILDING SPRAY INJECTION
REACTOR BUILDING COOLING SYSTEM (INJECTION PHASE)
EMERGENCY COOLANT INJECTION
REACTOR BUILDING SPRAY RECIRCULATION
REACTOR BUILDING COOLING SYSTEM (RECIRCULATION PHASE)
EMERGENCY COOLANT RECIRCULATION
SEQUENCE
RESULT
SEQ. #
B
K
C
Y
D
F
Z
H
KEY TO RESULTS
S - Safe condition expected (some fuel damage may result)
CM- Core melt expected
? - Possible core melt
3,11 from T-tree
16,21 from T-tree
SUCCESS
FAILURE
BKCYDFZH (B) S 1
BKCYDFZH (BH) CM 2
BKCYDFZH (BZ) S 3
BKCYDFZH (BZH) CM 4
BKCYDFZH (BF) S 5
BKCYDFZH (BFH) CM 6
BKCYDFZH (BFZ) ? 7
BKCYDFZH (BFZH) CM 8
BKCYDFZ (BD) CM 9
BKCYDFZ (BDZ) CM 10
BKCYDFZ (BDF) CM 11
BKCYDFZ (BDFZ) CM 12
BKCYDFH (BY) S 13
BKCYDFH (BYH) CM 14
BKCYDFH (BYF) ? 15
BKCYDFH (BYFH) CM 16
BKCYDF (BYD) CM 17
BKCYDF (BYDF) CM 18
BKCYDZH (BC) S 19
BKCYDZH (BCH) CM 20
BKCYDZH (BCZ) ? 21
BKCYDZH (BCZH) CM 22
BKCYDZ (BCD) CM 23
BKCYDZ (BCDZ) CM 24
BKCYDH (BCY) ? 25
BKCYDH (BCYH) CM 26
BKCYD (BCYD) CM 27
BK (BK) CM 28

Figure 4.3 LOCA Event Tree for Crystal River-3

Building Cooling System), removing radioactive effluents during injection (Reactor Building Spray Injection), keeping the core cooled during the recirculation phase of the LOCA (Emergency Coolant Recirculation), preventing containment overpressure during recirculation (Reactor Building Spray Recirculation and Reactor Building Cooling System), and removing radioactive effluents during recirculation (Reactor Building Spray Recirculation).

It may be recalled that the Reactor Safety Study included an event called emergency cooling functionability (ECF) on its large LOCA tree. This event represented those occasions when ECI operates, but the core is not cooled. This function is not included in the CR-3 trees.

The accident sequence symbology is analogous to that of the transient event tree; the symbol S with the appropriate subscript identifies the generic LOCA sequence. The initiating events are spontaneous LOCAs (B_1, B_2, B_3, or B_4) or one of the transients which progress to a LOCA. Examples of specific LOCA sequences are B_4S_{27} and T_{2A} T_{11} S_{27}.

The basic plant functions are always required, but the different LOCA sizes (and sometimes the particular location of the LOCA) determine equipment combinations required for success. Only two functions are affected by the break size: Subcriticality and core cooling. Subcriticality for the B_1, B_2 and B_3 LOCA results directly from the blowdown, but the B_4 LOCA requires operation of the RPS. Core cooling requirements change with break size and are a function of the RCS pressure response and the flow rate of the coolant being lost.

All of the systems/functions included in the event tree, and their failure criteria, are described in Table 4.5. As for the transient tree, emergency electric power was not included as an event tree function. The sodium hydroxide addition system is also not included.

BEST DOCUMENT AVAILABLE

Table 4.5 Event Definition for LOCA Event Tree

B LOCA - A breach of the pressure boundary of the reactor coolant system (RCS) which causes an uncontrollable loss of water inventory. There are four LOCA categories.

- Large LOCA (B_1) - a breach of the RCS with a flow area greater than 1 ft^2 (B_1 > 13.5" diameter).
- Medium LOCA (B_2) - a breach of the RCS with a flow area greater than .4 ft^2 and less than or equal to 1 ft^2 (13.5" $\geq B_2$ > 8.5" diameter).
- Small LOCA (B_3) - a breach of the RCS with a flow area greater than .087 ft^2 and less than or equal to .4 ft^2 (8.5" $\geq B_3$ > 4" diameter).
- Small-Small LOCA (B_4) - a breach of the RCS with a flow area less than or equal to .087 ft^2 (4" $\geq B_4$ diameter).

K Reactor Subcriticality - Failure of automatic (or manual) reactor scram by some time t_o; (Note: This event applies only to small-small LOCAs (B_4). For other LOCAs success is assumed due to the effects of blowdown.

C Reactor Building Spray Injection - Failure to provide flow from at least 1 of 2 reactor building spray pumps, taking suction from the BWST, through its respective spray header into the containment atmosphere.

Y Reactor Building Cooling System (Fans) (Injection Phase) - Failure to remove steam (heat) from the containment atmosphere by at least 1 out of 3 reactor building cooling fans.

D Emergency Coolant Injection - Failure to provide sufficient water to the core to prevent core melt during the injection phase.

- ECI for Large LOCA - failure to provide flow to the RCS from at least 1 out of 2 low pressure trains (taking suction from the BWST) and 2 out of 2 core flooding tanks.
- ECI for Medium LOCA - failure to provide flow to the RCS from (a) at least 1 out of 2 low pressure trains (taking suction from the BWST) and 2 out of 2 core flooding tanks, or (b) 2 out of 2 low pressure trains (taking suction from the BWST).
- ECI for Small LOCA - failure to provide flow to the RCS from at least 1 out of 2 high pressure trains and 1 out of 2 low pressure trains (taking suction from the BWST).
- ECI for Small-Small LOCA -
  - (a) For Sequences containing event $\bar{K}$ - failure to provide flow to the RCS from at least 1 out of 2 high pressure trains (taking suction from the BWST).
  - (b) For Sequences containing event K - failure to provide flow to the RCS from 2 out of 2 high pressure trains (taking suction from the BWST) and to provide flow to the secondary side of the steam generators from 1 out of 2 emergency feedwater trains.

F Reactor Building Spray Recirculation - Failure to provide flow from at least 1 out of 2 reactor building spray pumps, taking suction from the reactor building sump, through its respective spray header into the containment atmosphere for 24 hours.

Z Reactor Building Cooling System (Fans) (Recirculation Phase) - Failure to continue to remove steam (heat) from the containment atmosphere for 24 hours by at least 1 out of 3 reactor building cooling fans.

H Emergency Coolant Recirculation - Failure to provide sufficient water to the core to prevent core melt in the recirculation phase of a LOCA (24 hours).

- ECR for Large, Medium and Small LOCA - failure to provide flow to the RCS from (a) at least 1 out of 2 low pressure trains (taking suction from the reactor building sump) in conjunction with cooling by the associated Decay Heat Removal Subsystem or (b) at least 1 out of 2 low pressure trains (taking suction from the reactor building sump) in conjunction with cooling by at least 1 out of 3 Reactor Building Fan Coolers.
- ECR for Small-Small LOCA - failure to provide flow to the RCS from (a) at least 1 out of 2 high pressure trains with its associated low pressure train (taking suction from the reactor building sump) in conjunction with cooling by the associated Decay Heat Removal Subsystem or (b) at least 1 out of 2 high pressure trains with its associated low pressure train (taking suction from the reactor building sump) in conjunction with cooling by at least 1 out of 3 Reactor Building Fan Coolers.

The event tree was constructed by considering the various functionability/operability interrelationships between the systems/functions listed below:

1. Failure of Reactor Subcriticality (event K) is only possible during small-small LOCAs. This is because the rapid blowdown of the larger break sizes removes the moderator, shutting down the reaction, and the replacement coolant supplied by ECI is highly borated.
2. If Reactor Building Spray Injection fails (event C) then Reactor Building Spray Recirculation fails, since the most likely failures involve equipment which is common to both systems.
3. If the Reactor Building Cooling System fails during the injection phase (event Y), then it also fails during the recirculation phase, since the equipment used and the success criteria are exactly the same during both phases.
4. If Emergency Coolant Injection fails (event D), then Emergency Coolant Recirculation doesn't matter, since failure to provide sufficient injection phase cooling will result in a core melt regardless of what happens during the recirculation phase.

These interrelationships reduce the number of sequences from 128 to 28.

The equipment success requirements related to the functions defined in Table 4.5 and used in the definition of fault tree "top events" are shown in Table 4.6.

There are five nonmelt sequences, indicated on Figure 4.3 by the "S" in the Result column. For all these sequences, core melt is prevented by success of Reactor Subcriticality (shutting down the nuclear reaction), replacing the lost coolant by means of Emergency Coolant Injection, maintaining the water level above the core and removing decay heat by Emergency Coolant Recirculation, and preventing containment overpressure by the Reactor Building Spray System or the Reactor Building Cooling System.

There are four possible nonmelt sequences, indicated in Figure 4.3 by the "?" in the Result column. These sequences are similar to those mentioned above, except that containment overpressure is not prevented (both the Reactor Building Spray System and the Reactor Building Cooling System fail), resulting in containment overpressure and rapid flashing in the sump. Core melt will occur if this flashing causes the Emergency Coolant Recirculation pumps to cavitate and fail. Because there is substantial disagreement over the ability of these pumps to survive this scenario, these sequences are evaluated as core melts for the purposes of this report.

Table 4.6 Definition of ECCS Equipment Success Requirements for LOCA Events in Crystal River-3

LOCA SIZE	INJECTION PHASE			RECIRCULATION PHASE		
	CONTAINMENT OVERPRESSURE PROTECTION	POST ACCIDENT RADIOACTIVITY REMOVAL	EMERGENCY CORE COOLING	CONTAINMENT OVERPRESSURE PROTECTION	POST ACCIDENT RADIOACTIVITY REMOVAL	EMERGENCY CORE COOLING
0-4" (0-.087ft^2) B_4 LOCA	1/2 REACTOR BLDG. SPRAY INJECTION (RBSI) OR 1/3 REACTOR BLDG. FAN COOLER (RBCS)	1/2 RBSI ↓	1/3 HIGH PRESSURE INJECTION (HPIS) - - - - - - - - - - for $.008ft^2<D<.015ft^2$ 2/3 HPIS MAY BE REQUIRED	1/2 REACTOR BLDG SPRAY RECIRC. (RBSR) WITH LOW PRESSURE RECIRC. (LPRS) HEAT EXCHANGER OR 1/3 RBCS	1/2 RBSR ↓	1/3 HIGH PRESSURE RECIRC. (HPRS) W/ASSOCIATED LPRS TRAIN AND LPRS HEAT EXCHANGER
4"-8.5"D (.087-.4ft^2) B_3 LOCA	↓	↓	1/3 HPIS AND 1/2 LOW PRESSURE INJECTION (LPIS)	↓	↓	1/2 LPRS AND LPRS HEAT EXCHANGER OR 1/2 LPRS AND 1/3 RBCS
8.5"-13.5"D (.4-1.0ft^2) B_2 LOCA	↓	↓	2/2 LPIS OR 1/2 LPIS AND 2/2 CORE FLOOD TANKS (CFT) - - - - - - - - - - for CFT LINE BREAK 1/1 LPIS AND 1/1 CFT	↓	↓	↓ - - - - - - - - - - - for CFT BREAK 1/1 LPRS etc.
13.5"-36"D (1.0-7.1ft^2) B_1 LOCA	↓	↓	1/2 LPIS AND 2/2 CFT	↓	↓	↓

4.4 Special Events

This section presents the analyses of the last three initiating events indicated earlier in Section 4.1.

4.4.1 Interfacing Systems LOCA (Event V)

An interfacing systems LOCA is a breach of the highpressure reactor cooling system boundary at its interface with the low pressure cooling system; it results in primary coolant being discharged directly outside of the containment.[1] The potential for this event at Crystal River-3 was analyzed, and the event rejected as a signficant contributor to risk. The only locations susceptible to Event V are the low pressure injection lines which are connected to the reactor Coolant system piping. These are illustrated in Figure 4.4.

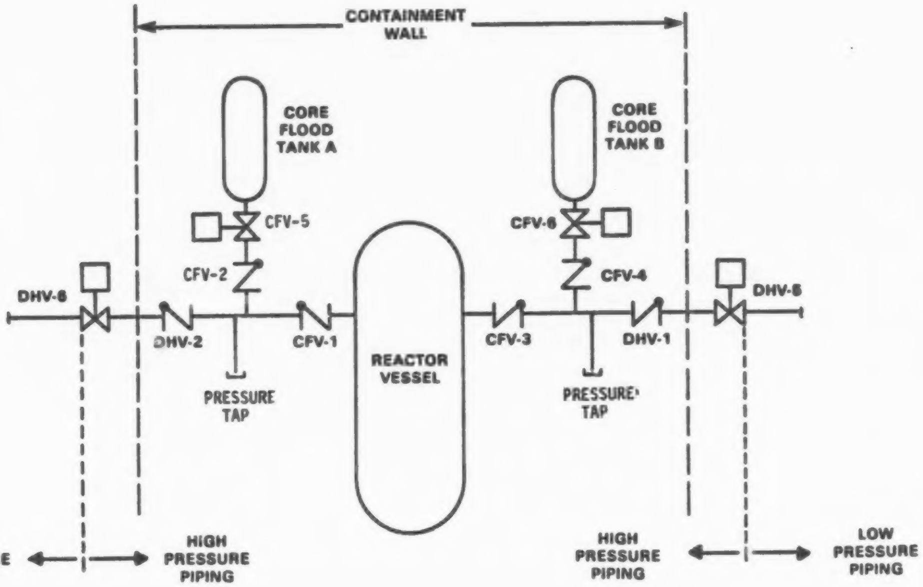

CONTAINMENT WALL
CORE FLOOD TANK A
CORE FLOOD TANK B
CFV-5
CFV-6
CFV-2
CFV-4
DHV-6
DHV-5
DHV-2
CFV-1
REACTOR VESSEL
CFV-3
DHV-1
PRESSURE TAP
PRESSURE TAP
LOW PRESSURE PIPING
HIGH PRESSURE PIPING
HIGH PRESSURE PIPING
LOW PRESSURE PIPING

FIGURE 4.4. INTERFACES BETWEEN REACTOR COOLANT SYSTEM AND LOW PRESSURE SYSTEMS

---

[1] This event is called Event V because it is analogous to the LOCA so designated in WASH-1400

In order to Event V to occur, the reactor coolant must flow through the protecting check valves CFV-3 and DHV-1 (or CFV-1 and DHV-2) and through the isolation valve just outside the containment wall, DHV-5 (or DHV-6), which will rupture the low pressure piping, cause the loss of primary coolant outside the containment, and result in an eventual core melt. For the sake of simplicity, the rest of the analysis is discussed in terms of the path through CFV-3, DHV-1, and DHV-5. The other path is symmetrical in every way, so that the total probability of Event V is twice the probability of the analyzed path.

A fault tree representing Event V for the analyzed path as constructed, taking into account the following information.

- During startup, the pressure between valves CFV-3 and DHV-1 is checked by means of a pressure tap located between the valves. pressure greater than 650 psi would indicate to the operator that CFV-3 has failed to reseat.
- A failure of valve DHV-1 to reseat during startup would result in loss of level and pressure in the core flood tank if the tank is properly aligned and functional. These conditions are alarmed to alert the operator.

The assumptions listed below concerning operator actions and system operations were made when the fault tree was constructed:

- The operator has the opportunity to close valve DHV-5 and isolate the break if he can diagnose the situation from available information within approximately 20 minutes.
- In the event that both DHV-1 and CFV-3 fail to reseat during startup, the reactor would trip before significant power levels had been reached, and the accident would be successfully averted. (The low pressure piping would rupture very early in startup since the RCS reaches its full operating pressure of 2200 psig at less than 15 percent power and the low pressure piping is designed for only 600 psig.)
- The plant goes all the way to cold shutdown once per year (to refuel) and it is at full pressure the rest of the time.

The result of the analysis is an estimated frequency of Event V of 2.0 E-9 per year, which is inconsequential for this study. The fault tree is shown in Figure 4.5 and the fault data is given in Table 4.7.

It is noted that there may be other locations where interfacing systems LOCAs may occur which may be of comparable significance to the very small frequency calculated for Event V; e.g., the residual heat removal suction lines. However, any initiating event of this type and order-of-magnitude would not be significant to the results of the study because of the much larger frequencies for ordinary LOCAs and transient events.

4.4.2 Vessel Rupture

A reactor vessel rupture event is defined as a vessel rupture large enough to negate the effectiveness of the emergency core cooling systems required to prevent core melt, or a rupture of sufficient primary coolant piping in a pattern that negates the effectiveness of those same systems. The potential for this event at Crystal River-3 was considered and rejected as a significant contributor to risk--for reasons similar to those described in Section 4.4.1 for rejecting the interfacing systems LOCA as a significant contributor to risk. The Reactor Safety Study assessed vessel rupture at 1.0 E-7/yr (median). Since probabilities of less than 1.0 E-7/yr were considered to be negligible in the present analysis (see Section 5) and we believe the Reactor Safety Study's value of 1.0 E-7/yr to be conservative, it was considered appropriate to eliminate vessel rupture from further consideration as an initiator.

It is noted that the possibility of reactor vessel rupture at pressure due to thermal shock, a subject of intense debate at the time of publication of this report, was outside the scope of the analysis and was not considered in this study.

BEST DOCUMENT AVAILABLE

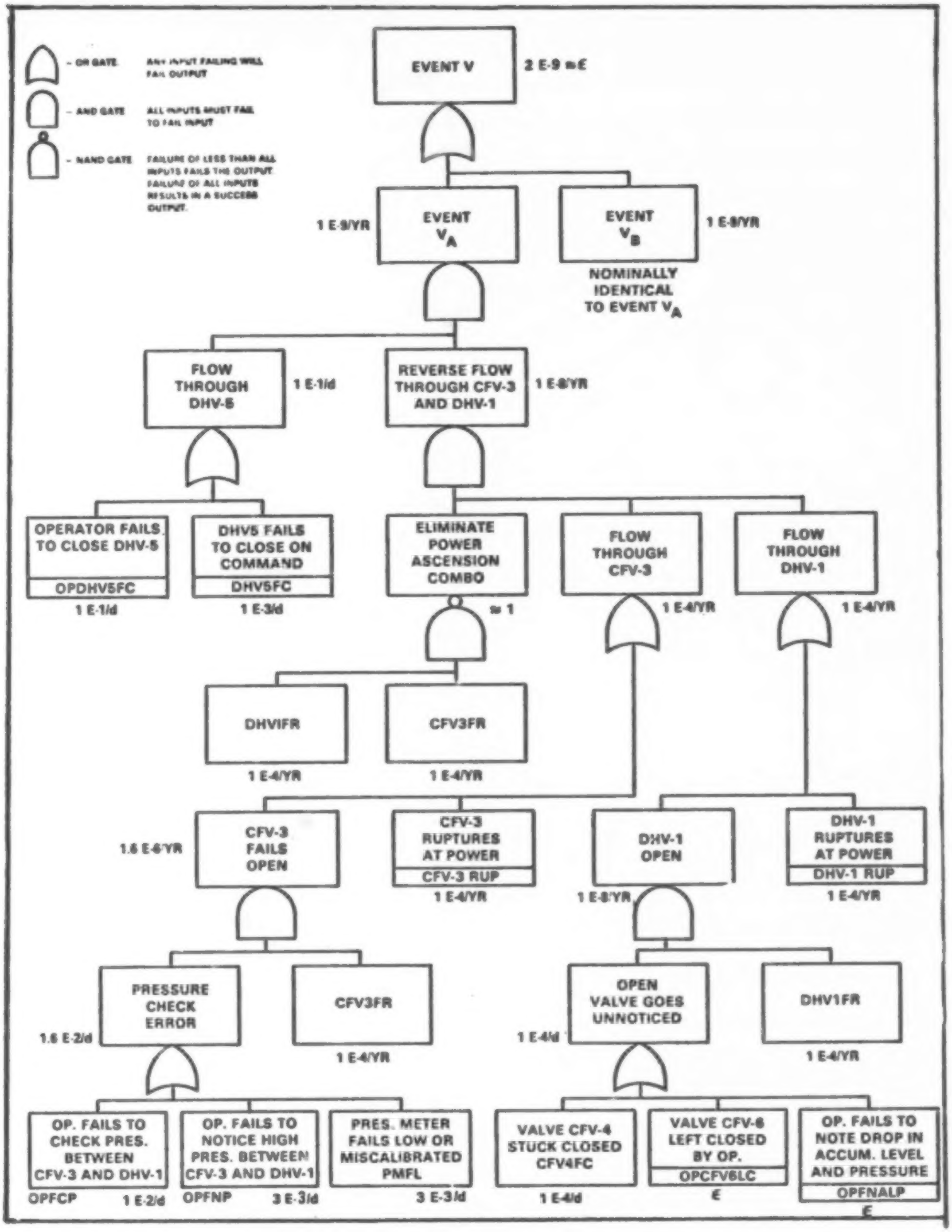

- OR GATE
ANY INPUT FAILING WILL FAIL OUTPUT
- AND GATE
ALL INPUTS MUST FAIL TO FAIL INPUT
- NAND GATE
FAILURE OF LESS THAN ALL INPUTS FAILS THE OUTPUT. FAILURE OF ALL INPUTS RESULTS IN A SUCCESS OUTPUT.
EVENT V
2 E-9 ≈ E
EVENT V_A
1 E-9/YR
EVENT V_B
1 E-9/YR
NOMINALLY IDENTICAL TO EVENT V_A
FLOW THROUGH DHV-5
1 E-1/d
REVERSE FLOW THROUGH CFV-3 AND DHV-1
1 E-8/YR
OPERATOR FAILS TO CLOSE DHV-5
OPDHV5FC
1 E-1/d
DHV5 FAILS TO CLOSE ON COMMAND
DHV5FC
1 E-3/d
ELIMINATE POWER ASCENSION COMBO
≈ 1
FLOW THROUGH CFV-3
1 E-4/YR
FLOW THROUGH DHV-1
1 E-4/YR
DHVIFR
1 E-4/YR
CFV3FR
1 E-4/YR
CFV-3 FAILS OPEN
1.6 E-6/YR
CFV-3 RUPTURES AT POWER
CFV-3 RUP
1 E-4/YR
DHV-1 OPEN
1 E-8/YR
DHV-1 RUPTURES AT POWER
DHV-1 RUP
1 E-4/YR
PRESSURE CHECK ERROR
1.6 E-2/d
CFV3FR
1 E-4/YR
OPEN VALVE GOES UNNOTICED
1 E-4/d
DHV1FR
1 E-4/YR
OP. FAILS TO CHECK PRES. BETWEEN CFV-3 AND DHV-1
OPFCP
1 E-2/d
OP. FAILS TO NOTICE HIGH PRES. BETWEEN CFV-3 AND DHV-1
OPFNP
3 E-3/d
PRES. METER FAILS LOW OR MISCALIBRATED
PMFL
3 E-3/d
VALVE CFV-4 STUCK CLOSED
CFV4FC
1 E-4/d
VALVE CFV-6 LEFT CLOSED BY OP.
OPCFV6LC
E
OP. FAILS TO NOTE DROP IN ACCUM. LEVEL AND PRESSURE
OPFNALP
E

FIGURE 4.5. FAULT TREE FOR EVENT V

BEST DOCUMENT AVAILABLE

Table 4.7 Fault Summary Sheet for Event V Fault Tree for Crystal River-3

FAULT	DESCRIPTION	DETECTION INTERVAL	COMMENTS	FAILURE RATE
CFV3FR, DHV1FR	check valve CFV-3 (DHV-1) fails to reseat during startup.	demand failure (1 demand/yr)	fault implies valve has been opened during shutdown because of low pressure systems check at refueling	1E-4/demand → 1 E-4/yr (failure to reseat assumed equal to failure to open)
CFV3RUP, DHV1RUP	check valve CFV-3 (DHV-1) ruptures while plant is at operating pressure, allowing backflow through the valve	~1 year at pressure (use 10^4 hrs)	the use of 10^4 hr between tests is highly conservative but covers the possibility of long operating times between tests. Detection of these ruptures between tests is assumed unlikely.	1E-8/hr → 1E-4/yr
CFV4FC	check valve CFV-4 (core flood tank "B" check valve) fails in the closed state, preventing flow from the tank.	demand failure	valve operability checked immediately prior to repressurizing for operation, thus valve would have to fail closed immediately after testing in order to prevent detection of stuck open DHV-1	1E-4/demand
OPDHV5FC	the operator fails to determine the cause of primary coolant loss and fails to close valve DHV-5 to isolate the loss	demand failure	operator has at least 20 min. (very conservative) to act. Most noticable indications would be high radiation alarms in selected areas of auxiliary building.	1E-1/demand
DHV5FC	valve DHV-5 fails to close given that the operator tries to close it	demand failure	valve design is sufficient to close at reactor operating pressure.	1E-3/demand
OPFCP	operator forgets to check the pressure between valves CFV-3 and DHV-1	demand failure	step included in startup procedure.	1E-2/demand
OPFNP	given that the pressure between CFV-3 and DHV-1 is high (CFV-3 has failed open) the operator fails to notice this when he performs the pressure check	demand failure	normal pressure should be be around 650 psi, faulted pressure would be around 2200 psi	3E-3/demand
PMFL	pressure meter used for check is failed low or miscalibrated	demand failure	same as above	3E-3/demand
OPCFV6LC	operator leaves valve CFV-6 (core flood tank isolation valve) closed after startup.	demand failure prompt detection (condition alarmed)	mentioned in at least 2 startup procedures. If valve closed as pressure increases above ~ 750 psi, condition is alarmed	ε
OPFNALP	given that DHV-1 is failed open and core flood tank (CFT) is properly lined up and functional, the operator fails to notice the decrease in CFT level and pressure	demand failure prompt detection	both low level and low pressure in CFT are alarmed	ε

4.4.3 Steam Generator Tube Rupture

A steam generator tube rupture is defined as a break in the interface between the primary and secondary systems in a steam generator. An examination of this initiator resulted in the determination that the basic plant behavior is similar to that for a loss of PCS transient, so that a separate evaluation is not required. This results from the following logic:

- The RCS is blowing down into the secondary system, which has a back pressure of about 900 psig. Blowdown therefore terminates at 900 psig instead of the 40 psig of a LOCA (which blows down to the containment), resulting in much less coolant being lost. Available information from the FSAR seems to indicate that the pressure will equalize before the core is uncovered and ECCS reflood will not be required.
- In order for the initiator to become a noncoolable LOCA, a relief valve in the secondary cooling system which cannot be isolated must fail to close. This requirement for an additional failure makes the entire sequence a low probability event.

Steam generator tube rupture is thus eliminated from consideration as a separate initiator.

4.5 Containment Failure Modes

The containment failure modes considered in this analysis are identical to those in WASH-1400. The five types, listed in Table 4.8 below, are briefly described in the following text. The reader who desires additional detail is referred to Appendix VIII of WASH-1400.

Table 4.8 Containment Failure Modes

Failure Mode	Symbol
Vessel Steam Explosion	α
Containment Leakage	β
Hydrogen Burning	γ
Overpressure	δ
Melt-through	ε

The five possible ways in which the containment can fail following a core melt accident sequence are considered in the event tree construction process. To minimize the complexity of the event tree, however, a separate tree is developed for the containment and subsequently combined with the accident sequences defined in the system level event tree. The containment event tree developed for CR-3, shown in Figure 4.6, is identical to the PWR containment event tree in WASH-1400.

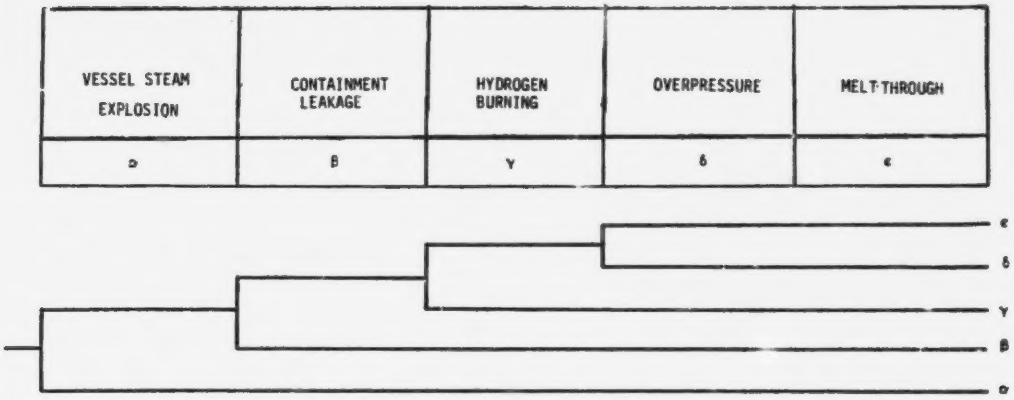


Figure 4.6 PWR Containment Event Tree (Ref. 4-1)

When the accident sequence and containment event trees are linked, it is necessary to consider the conditional dependencies that exist between the systems involved in each accident sequence and the containment, and to modify the containment tree for the various accident sequences. In other words, not all possible containment failure modes are possible for each accident sequence. For example, an accident sequence initiated by a small pipe break followed by success of emergency injection and recirculation would not involve consideration of containment rupture due to a steam explosion in the vessel since the reactor core was reflooded after the initiating event and emergency coolant recirculation (including residual heat removal) succeeded.

Linking of the function/system level event tree and the containment event tree results in defining the set of complete accident sequences for the particular initiating event being considered. Each complete sequence consists of a combination of an initiating event, a sequence of system failures, and a containment failure mode, e.g., B_4S_2-γ.

The five containment failure modes are briefly defined as follows:

α - Containment Rupture Due to Vessel Steam Explosion

A violent interaction between a large quantity of molten core material (UO_2) which falls into a pool of water remaining in the lower reactor vessel head results in a steam explosion in the vessel and rupture of the containment by large vessel fragments or the upper vessel head.

Serious consequences are possible from this containment failure mode because of the early containment failure and the early and energetic dispersal of the core into the containment atmosphere and the environment.

β - Containment Leakage

A leak rate from the containment large enough to preclude both hydrogen burning and containment failure by overpressurization.

WASH-1400 assumed that a leak rate of 200% per day, which is approximately equivalent to a hole in the containment 3.6 to 4 inches in diameter, was sufficient to meet this criterion.

γ - Containment Rupture Due to Hydrogen Burning

The combination of existing high pressure from steam and noncondensible gases (hydrogen and carbon dioxide) with energy generated by the burning of hydrogen in a core melt sequence near the end of the meltdown period results in a pressure increase sufficient to rupture containment.

The steam is generated by decay heat from the molten core; hydrogen is formed by water reacting with zirconium and steel; and carbon dioxide is formed by molten fuel interacting with the concrete in the containment floor.

δ - Containment Rupture Due to Overpressure

The buildup of pressure within the containment from steam and noncondensible gases (hydrogen and carbon dioxide) results in rupture of the containment.

ε - Containment Rupture Due to Meltthrough

The inevitable result of core melt, which will occur whether or not the containment was ruptured by another failure mode, or whether or not containment leakage prevented an overpressure rupture.

This failure mode is placed last on the containment event tree because it will generally occur last and not contribute significantly to consequences.

4.6 Radioactive Release Categories

The radioactive release categories utilized in the CR-3 evaluation are those defined in WASH-1400 for a PWR. We did not redefine or modify them in any way. Although nine release categories were defined in WASH-1400 for the PWR, only seven include accident sequences which result in core melt. These seven are the categories of interest to this study.

The categories are numbered PWR-1 through PWR-7, with PWR-1 having the most severe consequences and the others progressively less severe consequences, although the differences between categories are not easy to describe or quantify. The differences between categories are not constant or necessarily directly related due to the differences in the way they affect different types of consequences, e.g., short- or long-term health effects, land contamination, etc. A brief but moderately detailed description of the seven release categories of interest is provided in Table 4.9 for the convenience of the reader. An abridged discussion (from reference 4-5) which characterizes the release categories follows below. A more complete description and discussion of the release categories is contained in Appendix VI of WASH-1400 (Ref. 4-5). The reader is referred to that document for complete details.

"The release categories are generic classes of hypothetical accident sequences characterized by several parameters, the first of which is release magnitude. The others are time of release, duration of release, warning time for evacuation, height of release, and energy content of the released plume.

The time of release refers to the time interval between the start of the hypothetical accident and the release of radioactive material from the containment building to the atmosphere; it is used to calculate the initial decay of radioactivity. The duration of release is the total time during which radioactive material is emitted into the atmosphere; it is used to account for continuous releases by adjusting for horizontal dispersion due to wind meander. These parameters, time and duration of release, represent the temporal behavior of the release in the dispersion model. They are used to model a "puff" release from calculations of release versus time.

The warning time for evacuation is the interval between awareness of impending core melt and the release of radioactive material from the containment building. Finally, the height of release and the energy content of the released plume gas affect the manner in which the plume would be dispersed in the atmosphere.

Table 4.10 lists the leakage parameters that characterize the seven PWR release categories considered. It should be understood that these categories are composites of numerous event tree sequences with similar characteristics."

BEST DOCUMENT AVAILABLE

Table 4.9 PWR Category Descriptions (4-5)

PWR 1

This release category can be characterized by a core meltdown followed by a steam explosion on contact of molten fuel with the residual water in the reactor vessel. The containment spray and heat removal systems are also assumed to have failed and, therefore, the containment could be at a pressure above ambient at the time of the steam explosion. It is assumed that the steam explosion would rupture the upper portion of the reactor vessel and breach the containment barrier, with the result that a substantial amount of radioactivity might be released from the containment in a puff over a period of about 10 minutes. Due to the sweeping action of gases generated during containment-vessel meltthrough, the release of radioactive materials would continue at a relatively low rate thereafter. The total release would contain approximately 70% of the iodines and 40% of the alkali metals present in the core at the time of release.[1] Because the containment would contain hot pressurized gases at the time of failure, a relatively high release rate of sensible energy from the containment could be associated with this category. This category also includes certain potential accident sequences that would involve the occurrence of core melting and a steam explosion after containment rupture due to overpressure. In these sequences, the rate of energy release would be lower, although still relatively high.

PWR 2

This category is associated with the failure of core-cooling systems and core melting concurrent with the failure of containment spray and heat-removal systems. Failure of the containment barrier would occur through overpressure, causing a substantial fraction of the containment atmosphere to be released in a puff over a period of about 30 minutes. Due to the sweeping action of gases generated during containment vessel meltthrough, the release of radioactive material would continue at a relatively low rate thereafter. The total release would contain approximately 70% of the iodines and 50% of the alkali metals present in the core at the time of release. As in PWR release category 1, the high temperature and pressure within containment at the time of containment failure would result in a relatively high release rate of sensible energy from the containment.

PWR 3

This category involves an overpressure failure of the containment due to failure of containment heat removal. Containment failure would occur prior to the commencement of core melting. Core melting then would cause radioactive materials to be released through a ruptured containment barrier. Approximately 20% of the iodines and 20% of the alkali metals present in the core at the time of release would be released to the atmosphere. Most of the release would occur over a period of about 1.5 hours. The release of radioactive material from containment would be caused by the sweeping action of gases generated by the reaction of the molten fuel with concrete. Since these gases would be initially heated by contact with the melt, the rate of sensible energy release to the atmosphere would be moderately high.

PWR 4

This category involves failure of the core-cooling system and the containment spray injection system after a loss-of-coolant accident, together with a concurrent failure of the containment system to properly isolate. This would result in the release of 9% of the iodines and 4% of the alkali metals present in the core at the time of release. Most of the release would occur continuously over a period of 2 to 3 hours. Because the containment recirculation spray and heat-removal systems would operate to remove heat from the containment atmosphere during core melting, a relatively low rate of release of sensible energy would be associated with this category.

PWR 5

This category involves failure of the core cooling systems and is similar to PWR release category 4, except that the containment spray injection system would operate to further reduce the quantity of airborne radioactive material and to initially suppress containment temperature and pressure. The containment barrier would have a large leakage rate due to a concurrent failure of the containment system to properly isolate, and most of the radioactive material would be released continuously over a period of several hours. Approximately 3% of the iodines and 0.9% of the alkali metals present in the core would be released. Because of the operation of the containment heat-removal systems, the energy release rate would be low.

PWR 6

This category involves a core meltdown due to failure in the core cooling systems. The containment sprays would not operate, but the containment barrier would retain its integrity until the molten core proceeded to melt through the concrete containment base mat. The radioactive materials would be released into the ground, with some leakage to the atmosphere occurring upward through the ground. Direct leakage to the atmosphere would also occur at a low rate prior to containment-vessel meltthrough. Most of the release would occur continuously over a period of about 10 hours. The release would include approximately 0.08% of the iodines and alkali metals present in the core at the time of release. Because leakage from containment to the atmosphere would be low and gases escaping through the ground would be cooled by contact with the soil, the energy release rate would be very low.

PWR 7

This category is similar to PWR release category 6, except that containment sprays would operate to reduce the containment temperature and pressure as well as the amount of airborne radioactivity. The release would involve 0.002% of the iodines and 0.001% of the alkali metals present in the core at the time of release. Most of the release would occur over a period of 10 hours. As in PWR release category 6, the energy release rate would be very low.

---

[1] The release fractions of all the chemical species are listed in Table 4.10. The release fractions of iodine and alkali metals are indicated here to illustrate the variations in release with release category.

BEST DOCUMENT AVAILABLE

Table 4.10 Summary of Release Categories Representing Hypothetical Accidents (4-5)

Release Category	Probability (reactor-yr^{-1})	Time of Release (hr)	Duration of Release (hr)	Warning Time for Evacuation (hr)	Elevation of Release[g] (meters)	Energy Release (10^6 Btu/hr)	Fraction of Core Inventory Released[a]							
							Xe-Kr	Organic I[b]	I[b]	Cs-Rb	Te-Sb	Ba-Sr	Ru[c]	La[d]
PWR 1	9×10^{-7}[e]	2.5	0.5	1.0	25	20 and 520[e]	0.9	6×10^{-3}	0.7	0.4	0.4	0.05	0.4	3×10^{-3}
PWR 2	8×10^{-6}	2.5	0.5	1.0	0	170	0.9	7×10^{-3}	0.7	0.5	0.3	0.06	0.02	4×10^{-3}
PWR 3	4×10^{-6}	5.0	1.5	2.0	0	6	0.8	6×10^{-3}	0.2	0.2	0.3	0.02	0.03	3×10^{-3}
PWR 4	5×10^{-7}	2.0	3.0	2.0	0	1	0.6	2×10^{-3}	0.09	0.04	0.03	5×10^{-3}	3×10^{-3}	4×10^{-4}
PWR 5	7×10^{-7}	2.0	4.0	1.0	0	0.3	0.3	2×10^{-3}	0.03	9×10^{-3}	5×10^{-3}	1×10^{-3}	6×10^{-4}	7×10^{-5}
PWR 6	6×10^{-6}	12.0	10.0	1.0	0	N/A	0.3	2×10^{-3}	8×10^{-4}	8×10^{-4}	1×10^{-3}	9×10^{-5}	7×10^{-5}	1×10^{-5}
PWR 7	4×10^{-5}	10.0	10.0	1.0	0	N/A	6×10^{-3}	2×10^{-5}	2×10^{-5}	1×10^{-5}	2×10^{-5}	1×10^{-6}	1×10^{-6}	2×10^{-7}
PWR 8	4×10^{-5}	0.5	0.5	N/A[f]	0	N/A	2×10^{-3}	5×10^{-6}	1×10^{-4}	5×10^{-4}	1×10^{-6}	1×10^{-8}	0	0
PWR 9	4×10^{-4}	0.5	0.5	N/A	0	N/A	3×10^{-6}	7×10^{-9}	1×10^{-7}	6×10^{-7}	1×10^{-9}	1×10^{-11}	0	0
BWR 1	1×10^{-6}	2.0	0.5	1.5	25	130	1.0	7×10^{-3}	0.40	0.40	0.70	0.05	0.5	5×10^{-3}
BWR 2	6×10^{-6}	30.0	3.0	2.0	0	30	1.0	7×10^{-3}	0.90	0.50	0.30	0.10	0.03	4×10^{-3}
BWR 3	2×10^{-5}	30.0	3.0	2.0	25	20	1.0	7×10^{-3}	0.10	0.10	0.30	0.01	0.02	4×10^{-3}
BWR 4	2×10^{-6}	5.0	2.0	2.0	25	N/A	0.6	7×10^{-4}	8×10^{-4}	5×10^{-3}	4×10^{-3}	6×10^{-4}	6×10^{-4}	1×10^{-4}
BWR 5	1×10^{-4}	3.5	5.0	N/A	150	N/A	5×10^{-4}	2×10^{-9}	6×10^{-11}	4×10^{-9}	8×10^{-12}	8×10^{-14}	0	0

(a) Background on the isotope groups and release mechanisms is presented in Appendix VII.

(b) Organic iodine is combined with elemental iodines in the calculations. Any error is negligible since its release fraction is relatively small for all large release categories.

(c) Includes Ru, Rh, Co, Mo, Tc.

(d) Includes Y, La, Zr, Nb, Ce, Pr, Nd, Np, Pu, Am, Cm.

(e) Accident sequences within PWR 1 category have two distinct energy releases that affect consequences. PWR 1 category is subdivided into PWR 1A with a probability of 4×10^{-7} per reactor-year and 20×10^6 Btu/hr and PWR 1B with a probability of 5×10^{-7} per reactor-year and 520×10^6 Btu/hr.

(f) Not applicable.

(g) A 10 meter elevation is used in place of zero representing the mid-point of a potential containment break. Any impact on the results would be slight and conservative.

References

4-1 U.S. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

4-2 F. L. Leverenz, Jr., J. M, Koren, R. C. Erdmann, and G. S. Lellouche, Electric Power Research Institute, "ATWS: A Reappraisal, Part II Frequency of Anticipated Transients," EPRI NP-801, June 1978.

4-3 Florida Power Corporation, "Crystal River Unit 3 Nuclear Generating Plant Final Safety Analysis Report," Docket 50-302, 1971 (as amended through March 26, 1976).

4-4 U. S. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix III, WASH-1400 (NUREG-75/014), October 1975.

4-5 U.S. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," Appendix VI, WASH-1400 (NUREG-75/014), October 1975.

5.0 FAULT AND EVENT TREE QUANTIFICATION PROCEDURES

An overview of the fault tree analyses of Crystal River-3 is provided in this chapter. The analytical techniques, the basic assumptions and the sources of data used in obtaining point estimates of safety system unavailabilities are described first. With a few exceptions, the basic approach is the same as that used in the Reactor Safety Study (5-1). The second section outlines the organization and structure of the Crystal River fault trees and gives some intermediate results. It also serves as a guide to the appendices which contain the bulk of the analysis and results pertaining to individual systems. Next, the procedures for analyzing accident sequences are discussed and the results are presented. Finally, the detailed analysis of a selected set of operator faults is discussed.

5.1 ANALYTICAL METHODS FOR ESTIMATING PRIMARY EVENT PROBABILITIES

Point estimates of CR-3 safety system unavailability or unreliability were obtained. Single failures, and active double component failures that would fail the system were quantified, as were operator and human faults, test and maintenance outages, and failures of supporting systems, such as AC and DC power, which would contribute to safety unavailability.

5.1.1 FAULT TREE DEVELOPMENT

Detailed fault trees were developed for each system to a level of detail sufficient to identify possible common mode or common-cause failures. Simplified fault trees were then developed from the detailed trees. The simplified trees contained only single active and passive faults, double active faults, test and maintenance outages, and common mode failures. The faults appearing on the simplified fault trees were then grouped by type into modules to aid in the quantification of the event tree sequences. Each module consists of one or more faults, usually under an OR gate.[1] The modules were constructed to be completely independent of each other. That is, all faults appearing in a particular module appear in no other modules on any fault tree, although a module may itself appear in more than one fault tree. The intent in constructing the modules was to collect the maximum number of faults under a particular OR gate such that the module remained independent of all other modules. For example, on any one tree separate modules would be constructed for single hardware faults that appear in only one system and for single hardware faults that appear in more than one system. The faults on each side of a double would be collected into two separate modules. Operator errors were each expressed as separate modules for the sake of visibility. Interfacing system faults were expressed as separate modules for each train of the interfacing system (i.e., AC power was modularized as ACA and ACB, for AC train A and AC train B, respectively).

---

[1] Boolean algebra operations discussed in the text are written in capital letters and underlined, e.g., OR, AND, to eliminate possible logical ambiguity with text.

Construction of modularized fault trees reduced the number of terms in the Boolean equation representing the fault tree and resulted in a tractable Boolean reduction effort to evaluate the event tree sequences. Even so, a Boolean reduction computer code was required (5-2).

The types of modules contained in a typical tree are illustrated in the generic modularized fault tree presented in Figure 5.1. These modules and their evaluation are described in the following paragraphs. The single hardware failures generally did not contribute to safety system unavailability. Single failures generally consisted of pipe or tank ruptures with very small failure rates; in many instances failure modes are monitored. The NRC single failure criterion generally prohibits single failures that would result in safety system failure.

Individual train faults or outages were partitioned into at least four categories, as shown in Figure 5.1. These four categories are: a) single faults, both hardware and human, that fail a train; b) maintenance outages that leave a train unavailable or result in a less redundant system for the duration of maintenance; c) test outages that remove a train from service for the test duration; and d) interfacing system faults that fail a train, such as faults in the corresponding trains of AC power, DC power, or component cooling.

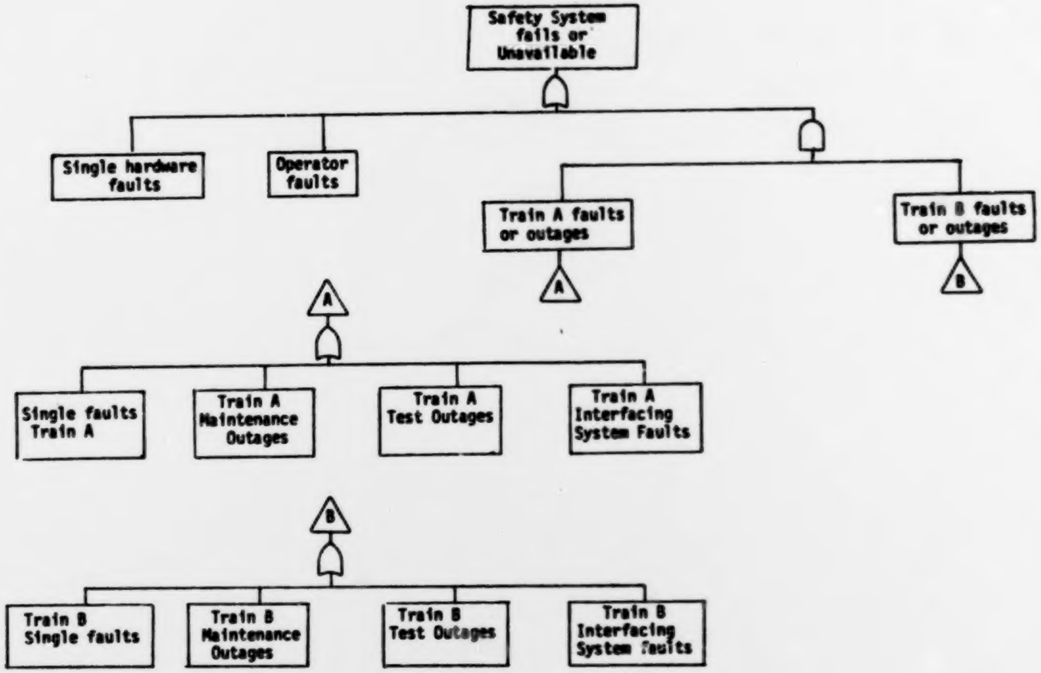

Safety System fails or Unavailable
Single hardware faults
Operator faults
Train A faults or outages
Train B faults or outages
A
B
A
Single faults Train A
Train A Maintenance Outages
Train A Test Outages
Train A Interfacing System Faults
B
Train B Single faults
Train B Maintenance Outages
Train B Test Outages
Train B Interfacing System faults

Figure 5.1 Generic Modularized Fault Tree for "Safety System Fails or Unavailable"

BEST DOCUMENT AVAILABLE

5.1.2 QUANTIFICATION DATA BASE

The principal data base employed in the Crystal River-3 analysis for component failure rates was the IREP data base (5-3). With the exception of failure rates for safety valves and turbine-driven pumps, this data is taken from WASH-1400 (5-1). The data is reproduced here in Tables 5.1a and 5.1b.

Use of plant specific data was considered for: (1) emergency power from the on-site fossil units 1 and 2; (2) emergency diesel generators; (3) emergency feedwater turbine pump; (4) batteries, and; (5) maintenance outage frequency and duration of active mechanical components. Each of these are described below.

Emergency AC Power from Units 1 and 2

Examination of the operating availability history for CR-1 and CR-2 from the EEI data shown in Table 5.2 yields availability figures of .827 and .848 respectively (5-4). Based on this limited information, availabilities of 80% (or 20% unavailability) were used for each unit.

Information from the plant also indicates that there have been two occurrences of loss of offsite power during the period when the fossil units were in operation and before CR-3 came on-line. On each of these occurrences, one of the fossil units (not the same one) tripped while the other ran back and stayed on-line. Based on this very limited sample, we have estimated a probability of 0.5 for each fossil unit failing to successfully run back and stay on-line when off-site power is lost.

Emergency Diesel Generators

The WASH-1400 diesel demand failure probability of 3E-2/d was used for the initial CR-3 accident sequence assessments. Because diesel failure appears in dominant cut sets of dominant accident sequences, plant specific data were reviewed for diesel failure Licensee Event Reports indicate 6 failures to start in 213 demands, yielding an estimated failure propability of 2.8E-3/demand. For practical purposes, this is essentially identical to the IREP/WASH-1400 figure, which was therefore used in the final analyses.

The possibility of non-independent diesel failure probabilities is discussed later in connection with the common-cause data base.

Table 5.1a Mechnical Component Failure Rate Data (from WASH-1400, Table III 4-1)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE		MEDIAN	EF	
PUMPS (INCLUDES DRIVER):						
MOTOR & TURBINE DRIVEN (GENERIC CLASS):						
FAILURE TO START ON DEMAND:	D (A)	3E-4	3E-3	1E-3	3	
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENTS):	O	3E-6	3E-4	3E-5	10	
FAILURE TO RUN, GIVEN START, (EXTREME, POST ACCIDENT ENVIRONMENTS INSIDE CONTAINMENT)	O	1E-4	1E-2	1E-3	10	
FAILURE TO RUN, GIVEN START (POST ACCIDENT, AFTER ENVIRONMENTAL RECOVERY)	O	3E-5	3E-3	3E-4	10	
TURBINE DRIVEN PUMPS:						
FAILURE TO START ON DEMAND:	D	1E-3	1E-2	3E-3	3	A
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT)	O	1E-5	1E-4	3E-5	3	A
VALVES:						
MOTOR OPERATED:						
FAILURE TO OPERATE (INCLUDES DRIVER):	D (B)	3E-4	3E-3	1E-3	3	
FAILURE TO REMAIN OPEN (PLUG):	D (C)	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG):	S	1E-7	1E-6	3E-7	3	
RUPTURE	S	1E-9	1E-7	1E-8	10	
SOLENOID OPERATED:						
FAILURE TO OPERATE:	D (D)	3E-4	3E-3	1E-3	3	
FAILURE TO REMAIN OPEN (PLUG):	D	3E-5	3E-4	1E-4	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
AIR-FLUID OPERATED:						
FAILURE TO OPERATE:	D (B)	1E-4	1E-3	3E-4	3	
FAILURE TO REMAIN OPEN (PLUG).	D	3E-5	3E-4	1E-4	3	
FAILURE TO REMAIN OPEN (PLUG).	S	1E-7	1E-6	3E-7	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
CHECK VALVES:						
FAILURE TO OPEN:	D	3E-5	3E-4	1E-4	3	
INTERNAL LEAK (SEVERE):	D	1E-7	1E-6	3E-7	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
VACUUM VALVE:						
FAILURE TO OPERATE:	D	1E-5	1E-4	3E-5	3	
MANUAL VALVE:						
FAILURE TO OPERATE:	D	3E-5	3E-4	1E-4	3	A
FAILURE TO REMAIN OPEN (PLUG):	D	3E-5	3E-4	1E-4	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
PRIMARY SAFETY VALVES (PWR):						
FAIL TO OPEN:	D	1E-3	1E-2	3E-3	3	R
PREMATURE OPEN:	S	1E-6	1E-5	3E-6	3	R
FAIL TO RECLOSE (GIVEN VALVE OPEN):	D (E)	3E-3	3E-2	1E-2	3	R
PRIMARY SAFETY VALVES (BWR):						
FAIL TO OPEN:	D	3E-3	3E-2	1E-2	3	R
PREMATURE OPEN:	S	1E-6	1E-5	3E-6	3	R
FAIL TO RECLOSE (GIVEN VALVE OPEN):	D	1E-3	1E-2	3E-3	3	R
TEST VALVES, FLOW METERS, ORIFICES:						
FAILURE TO REMAIN OPEN (PLUG):	D	1E-4	1E-3	3E-4	3	
RUPTURE:	S	1E-9	1E-7	1E-8	10	
PIPES						
PIPE ≤ 3-INCH DIAMETER (PER SECTION): RUPTURE/PLUG:	S + O	3E-11	3E-8	1E-9	30	
PIPE > 3-INCH DIAMETER (PER SECTION): RUPTURE/PLUG	S + O	3E-12	3E-9	1E-10	30	
CLUTCH, MECHANICAL:						
FAILURE TO OPERATE:	D (D)	1E-4	1E-3	3E-4	3	
SCRAM RODS (SINGLE):						
FAILURE TO INSERT:	D	3E-5	3E-4	1E-4	3	

NOTES:

(A) DEMAND PROBABILITIES ARE BASED ON THE PRESENCE OF PROPER INPUT CONTROL SIGNALS. FOR TURBINE DRIVEN PUMPS THE EFFECT OF FAILURES OF VALVES, SENSORS AND OTHER AUXILIARY HARDWARE MAY RESULT IN SIGNIFICANTLY HIGHER OVERALL FAILURE RATES FOR TURBINE DRIVEN PUMP SYSTEMS.

(B) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.

(C) PLUG PROBABILITIES ARE GIVEN IN DEMAND PROBABILITY, AND PER HOUR RATES, SINCE PHENOMENA ARE GENERALLY TIME DEPENDENT, BUT PLUGGED CONDITION MAY ONLY BE DETECTED UPON A DEMAND OF THE SYSTEM.

(D) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.

(E) THESE RATES ARE BASED ON LER'S FOR B&W PRESSURIZER PORV FAILURE TO RESEAT GIVEN THE VALVE HAS OPENED.

ABBREVIATIONS:

(1) FOR FAILURE RATE TYPE ABBREVIATIONS:

D = DEMAND FAILURE RATE - FAILURES PER DEMAND
O = OPERATING FAILURE RATE - FAILURES PER HOUR OF OPERATION
S = STANDBY FAILURE RATE - FAILURES PER HOUR OF STANDBY
S + O = STANDBY OR OPERATING FAILURE RATE - FAILURES PER HOUR

(2) REMARKS (LAST COLUMN) ABBREVIATIONS:

R = FAILURE RATE SHOWN IS A REVISION OF WASH-1400 VALUE
A = FAILURE RATE SHOWN IS IN ADDITION TO WASH-1400 FAILURE RATES

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table 5.1b Electrical Component Failure Rate Data (from WASH-1400, Table III 4-2)

COMPONENT & FAILURE MODE	FAILURE RATE TYPE	ASSESSED RANGE	MEDIAN	EF
CLUTCH, ELECTRICAL:				
FAILURE TO OPERATE:	D (a)	1E-4 1E-3	3E-4	3
PREMATURE DISENGAGEMENT:	O	1E-7 1E-5	1E-6	10
MOTORS, ELECTRIC:				
FAILURE TO START:	D (a)	1E-4 1E-3	3E-4	3
FAILURE TO RUN, GIVEN START (NORMAL ENVIRONMENT):	O	3E-6 3E-5	1E-5	3
FAILURE TO RUN, GIVEN START (EXTREME ENVIRONMENT):	O	1E-4 1E-2	1E-3	10
RELAYS:				
FAILURE TO ENERGIZE	D (a)	3E-5 3E-4	1E-4	3
FAILURE OF NO CONTACTS TO CLOSE, GIVEN ENERGIZED:	O	1E-7 1E-6	3E-7	3
FAILURE OF NO CONTACTS BY OPENING, GIVEN NOT ENERGIZED:	O	3E-8 3E-7	1E-7	3
SHORT ACROSS NO/NO CONTACT:	O	1E-9 1E-7	1E-8	10
COIL OPEN:	O	1E-8 1E-6	1E-7	10
COIL SHORT TO POWER:	O	1E-9 1E-7	1E-8	10
CIRCUIT BREAKERS:				
FAILURE TO TRANSFER:	D (a)	3E-4 3E-3	1E-3	3
PREMATURE TRANSFER:	O	3E-7 3E-6	1E-6	3
SWITCHES:				
LIMIT:				
FAILURE TO OPERATE:	D	1E-4 1E-3	3E-4	3
TORQUE:				
FAILURE TO OPERATE:	D	3E-5 3E-4	1E-4	3
PRESSURE:				
FAILURE TO OPERATE:	D	3E-5 3E-4	1E-4	3
MANUAL:				
FAILURE TO TRANSFER:	D	3E-6 3E-5	1E-5	3
SWITCH CONTACTS:				
FAILURE OF NO CONTACTS TO CLOSE GIVEN SWITCH OPERATION:	O	1E-8 1E-6	1E-7	10
FAILURE OF NC BY OPENING, GIVEN NO SWITCH OPERATION:	O	3E-9 3E-7	3E-8	10
SHORT ACROSS NO/NC CONTACT:	O	1E-9 1E-7	1E-8	10
BATTERY POWER SYSTEM (WET CELL):				
FAILURE TO PROVIDE PROPER OUTPUT:	S	1E-6 1E-5	3E-6	3
TRANSFORMERS:				
OPEN CIRCUIT PRIMARY OR SECONDARY:	O	3E-7 3E-6	1E-6	3
SHORT PRIMARY TO SECONDARY:	O	3E-7 3E-6	1E-6	3
SOLID STATE DEVICES, HIPOWER APPLICATIONS (DIODES, TRANSISTORS, ETC.):				
FAILS TO FUNCTION:	O	3E-7 3E-5	3E-6	10
FAILS SHORTED:	O	1E-7 1E-5	1E-6	10
SOLID STATE DEVICES, LOW POWER APPLICATIONS:				
FAILS TO FUNCTION:	O	1E-7 1E-5	1E-6	10
FAILS SHORTED:	O	1E-8 1E-6	1E-7	10
DIESELS (COMPLETE PLANT):				
FAILURE TO START:	D	1E-2 1E-1	3E-2	3
FAILURE TO RUN, EMERGENCY CONDITIONS, GIVEN START:	O	3E-4 3E-2	3E-3	10
DIESELS (ENGINE ONLY):				
FAILURE TO RUN, EMERGENCY CONDITIONS, GIVEN START	O	3E-5 3E-3	3E-4	10
INSTRUMENTATION - GENERAL (INCLUDES TRANSMITTER, AMPLIFIER AND OUTPUT DEVICE):				
FAILURE TO OPERATE:	O	1E-7 1E-5	1E-6	10
SHIFT IN CALIBRATION:	O	3E-6 3E-4	3E-5	10
FUSES:				
FAILURE TO OPEN:	D	3E-6 3E-5	1E-5	3
PREMATURE OPEN:	O	3E-7 3E-6	1E-6	3
WIRES (TYPICAL CIRCUITS, SEVERAL JOINTS):				
OPEN CIRCUIT:	O	1E-6 1E-5	3E-6	3
SHORT TO GROUND:	O	3E-8 3E-6	3E-7	10
SHORT TO POWER:	O	1E-9 1E-7	1E-8	10
TERMINAL BOARDS:				
OPEN CONNECTION:	O	1E-8 1E-6	1E-7	10
SHORT TO ADJACENT CIRCUIT:	O	1E-9 1E-7	1E-8	10

NOTES

(A) DEMAND PROBABILITIES ARE BASED ON PRESENCE OF PROPER INPUT CONTROL SIGNALS.

ABBREVIATIONS:

(1) FOR FAILURE RATE TYPE ABBREVIATIONS:
D = DEMAND FAILURE RATE - FAILURES PER DEMAND
O = OPERATING FAILURE RATE - FAILURES PER HOUR OF OPERATION
S = STANDBY FAILURE RATE - FAILURES PER HOUR OF STANDBY
S + O = STANDBY OR OPERATING FAILURE RATE - FAILURES PER HOUR

(2) REMARKS (LAST COLUMN) ABBREVIATIONS:
R = FAILURE RATE SHOWN IS A REVISION OF WASH-1400 VALUE
A = FAILURE RATE SHOWN IS IN ADDITION TO WASH-1400 FAILURE RATES

Table 5.2 Operating Availability History Data[1] for Crystal River Units 1 and 2

		Operating Availability (%)	
Year	Fuel	CR-1	CR-2
1967	coal	89.1	
1968	coal	78.0	
1969	coal	86.6	
1970	coal	66.0	89.3
1971	coal	90.8	74.4
1972	coal	83.9	88.3
1973	oil	85.3	76.4
1974	oil	79.4	92.5
1975	oil	85.3	88.0
		Avg = 82.7	Avg= 84.8

[1] Source: Edison Electric Institute, Reference 5-4

Emergency Feedwater Turbine Pump

The WASH-1400 data base does not distinquish turbine pump faults from failures of other kinds of pumps. Turbine pumps faults are, however, given in NUREG/CR-1205 (5-5). This reference gives a value of 2E-2 as the failure-to-start probability for turbine pumps used in B&W plants. This is approximately an order of magnitude larger than the pump failure-to-start probability given in the WASH-1400 data base. The CR-3 plant-specific data presented in NUREG/CR-1205 indicates 6 failures out of 15 turbine pump demands, which would give an estimated failure-to-start probability of 0.4. However, this plant specific number is considered too high for several reasons:

- The estimated number of demands (15) is probably smaller than the number which actually occurred. The number supposedly includes only those demands explicitly required by technical specifications
- The number of failures probably reflects a significant burn-in effect, whereas our analysis is intended to represent a steady state condition of the plant
- The relatively small number of demands could lead to a significant deviation from the mean value of turbine pump failure probability.

Based on these considerations, it was decided to use the more generic turbine pump failure-to-start probability of 2E-2 for B&W plants, which includes the CR-3 experience. It is believed that this number more closely represents the steady state turbine pump failure probability for CR-3 than the plant specific value estimated from the incomplete data. which does not fit our modeling assumptions.

Batteries

Battery faults also appear in dominant cut sets of dominant accident sequences. The original sequence evaluation used the IREP/WASH-1400 battery failure rate, which is derived primarily from lead-acid battery history. The CR-3 batteries are of the lead-calcium type. Insufficient plant-specific data were available from CR-3 battery history (approximately 2 years of operating history) to estimate a failure rate for the CR-3 lead-calcium batteries, but some general data were located (5-6,5-7) that indicated the failure rate of lead-calcium batteries is essentially the same as the rate given by IREP/WASH-1400 for lead-acid batteries; this value was therefore used.

Maintenance Outage Frequency and Duration

Plant-specific data on scheduled maintenance frequency and outage duration for major active components were obtained by written communication from the plant (5-8,5-9). These data suggest an average frequency of scheduled maintenance of about 2.0E-2 acts per month per component in emergency core cooling systems and about once per quarter per train for the emergency feedwater system. Average outage durations are approximately 7 hours for valves and 19 hours for pumps. Diesel maintenance is not scheduled while the reactor is operating and therefore does not contribute to unavailability.

Unscheduled maintenance contributions are negligible and were not individually assessed.

Human Error Data Base

The basic data base used for the assessment of human and operator errors was taken from WASH-1400, and augmented by subsequent further analyses of operator errors appearing in dominant cut sets of dominant accident sequences. The CR-3 analysis distinguished between human errors that occur during routine operation, such as leaving valves in an incorrect position after test and maintenance, and operator errors committed during the course of an accident in attempting to mitigate the accident. For the initial sequence evaluation, operator errors were assessed to be 0.1, 0.01 or 0.001 per act, depending on the stress factors that were expected to exist for the operations in question, and depending on an initial evaluation of the procedures pertaining to the act. For operator errors that appeared in dominant accident sequences, THERP (Technique for Human Error Rate Prediction) trees were constructed and analyzed using human error data from NUREG/CR-1278 (5-10). These analyses are discussed later in Section 5.4.

The assessment of common mode double human errors was generally performed using a β-factor, for coupled errors, of 0.1. The β-factor is the conditional probability of the second error, given the first. This differs from the root mean square method employed in WASH-1400, although the numerical results are similar.

Common-Cause Data Base

Certain valves and pumps on redundant trains of systems were assessed assuming coupled (non-independent) failure probabilities. In the initial assessment, to obtain an order-of-magnitude indication of the impact of common-cause, a β-factor of 0.1 was used throughout to couple pumps and valves with potential common-cause failure modes. This value of the β-factor was based on information in reference 5-11.

Prior to the final analysis, references 5-12 and 5-13 were reviewed, and the information incorporated into the final common-cause analysis. Reference 5-12 indicates that diesel failures appear to be essentially uncoupled, and therefore the final CR-3 diesel assessment was performed assuming no contribution from common-cause failures of both diesels. The β-factor for common-cause failures of pumps in redundant trains, and for major valves in redundant trains, was assigned as 0.1 for the final analysis. This value is in line with reference 5-11, and is within the error bounds of the information contained in reference 5-12

Procedures and Technical Specifications

The CR-3 procedures[1] and Technical Specifications (5-14) were reviewed and information contained therein was used as part of the analytical data base. Procedures, as well as information obtained on plant visits, were used to assist in assessing human errors. The plant surveillance requirements were used to obtain component test periods to assess the test outage contributions, and to assess component unavailabilities having per hour failure rates. (Per demand component failure probabilities were used directly from Table 5.1). Actual plant surveillance practice was incorporated into the analysis for diesel generator testing, since the plant tests these components more often than the Technical Specifications require.

---

[1] The procedures types used in the analysis included operating (OP-series), emergency (EP-series), abnormal (AP-series), maintenance (MP-and PM-series), and surveillance (SP-series) procedures

5.1.3 EVALUATION OF HARDWARE FAULTS

Point estimates of component hardware unavailabilities were evaluated assuming exponentially distributed times between failures. Fault duration times of one-half the test period were used throughout to estimate average unavailability. It was assumed that tests involve an entire train, so that every component in the train is tested. Unavailability point estimates q_c, for components having per hour failure rates were evaluated as:

$$q_c = \frac{1}{T}\int_0^T (1 - e^{-\lambda t})dt \approx \lambda T/2$$

where: q_c = component average unavailability
λ = component failure rate (per hour)
T = period between tests of the component (hours)

The above approximate expression for q_c is valid for values of $\lambda T/2 < 0.1$, which was always the case. For component failure modes whose failure rates are more appropriately expressed in terms of cyclic failure (per demand), such as "pump fails to start" or "valve fails to change position," the demand failure probability data in Table 5.1 were used without modification.

5.1.4 EVALUATION OF HUMAN FAULTS

A distinction was made in this analysis between operator errors and human errors. Operator errors are defined as errors involving direct and active misoperation of a safety system (e.g., incorrectly terminating the high pressure injection when HPI is required). Operator errors were shown on the modularized fault trees as separate items. Human errors are defined as errors occurring during routine operation, such as leaving valves in the wrong position after test or maintenance. Coupled human errors that would fail both trains of a safety system were grouped with the single faults on the individual trains.

Factors used to guide the quantification of operator errors included a review of operating procedures applicable to mitigating the accident, a review of other operations that the operator is required to perform concurrently with the operation being assessed, chances for recovery from the error, and additional information obtained from discussions with plant personnel.

For the initial assessment, operator errors were assessed on an order-of-magnitude basis. A basic operator error rate of 1.0 E-2 was assumed as the starting point. This rate was adjusted up or down by an order-of-magnitude depending on the expected influence of the other factors considered. A more detailed analysis using THERP trees was performed to quantify those operator errors found to be quantitatively significant in the dominant accident sequences. Each of the THERP trees developed and analyzed is described in Section 5.4.

Human errors committed during routine operation were categorized as "single faults" within individual trains and were coupled, if appropriate, when the Boolean equation for the fault tree was derived. In most cases these faults involved leaving valves in an incorrect position after test or maintenance. The probability of leaving a single valve in the wrong position was assumed to be 1.0 E-2 per act (from WASH-1400). This probability was used throughout the present analysis for this type of human error. A coupling coefficient of 0.1 was used for the conditional probability of also leaving the corresponding valve in the other train in the wrong position, given the first act. (A few special cases are treated individually as they arise.) However, this conditional probability was used only for those cases where the trains are tested or maintained sequentially. Staggered testing is performed on redundant subsystem trains in most cases so that human errors of this type do not contribute significantly to safety system unavailability. (CR-3 uses standard Technical Specification, which specify staggard testing.)

5.1.5 EVALUATION OF COMMON-CAUSE FAULTS

Certain hardware faults on each of two redundant trains were assumed to be coupled. These cross-train coupled hardware faults were also included in the "single faults" category on each train and were coupled when the Boolean equation for the fault tree was derived. The β-factor, or conditional probability of failure approach, was used to assess coupled hardware faults. Not every major cross-train component pair was assumed to have coupled failure modes. Only major pumps and valve pairs (generally at an interface with another system) being exposed to conditions with potential for failing both components were assessed for common-cause failures. A β-factor of 0.1 was used throughout, where coupling was assumed, for the conditional probability that the second pump or valve fails, given that the first failed.

5.1.6 EVALUATION OF TEST AND MAINTENANCE OUTAGES

Scheduled maintenance outage contributions to single train unavailability were assessed for pumps and motor-operated valves that undergo scheduled maintenance during normal plant operation. The maintenance contribution to single train unavailability for a component in that train, q_m, was assessed as:

$$q_m = \frac{f.t_m}{720}$$

where: f = frequency at which scheduled maintenance is performed (acts/month; f/720=acts/hour)

t_m = average outage time per maintenance act (hours)

Only major components on which maintenance can be performed without violation of Technical Specifications or reasonable safety constraints were assumed to be maintained when the reactor is operating.

Maintenance contributions to the unavailability of each train were assessed and then combined in the Boolean equation representing system failure. Cross-maintenance terms, representing simultaneous outage of both trains, were removed from the Boolean equation since this is prohibited by Technical Specifications. Terms representing maintenance of one train at the same time that the other train is out for test were also removed for the same reason. This is not to say that Technical Specifications are never violated. But we expect, and therefore assume, the probability of these events is small compared to the total unavailabilitites.

Test outage contributions to single train unavailability were assessed for tests that removed the entire train from service. The test times used throughout were those assumed in WASH-1400. Test frequencies were obtained from the CR-3 surveillance requirements (5-14) for each safety system.

The test contribution to single train unavailability, q_t, was assessed as:

$$q_t = \frac{t_T}{P}$$

where: t_T = single train outage time per test (hours)

P = test period (time between tests of the train)(hours)

Test contributions to the unavailability of each train were assessed and then combined in the Boolean equation representing system unavailability. As in the assessment of maintenance contributions, cross-test terms representing simultaneous outages of both trains were removed from the Boolean equation since this is prohibited by Technical Specifications. Terms representing test outages in one train at the same time that the other train is out for maintenance were also removed for the same reason.

5.1.7 EVALUATION OF INTERFACING SYSTEM FAULTS

Interfacing system fault contributions to safety system single train unavailabilities were assessed where they resulted from the failure of AC power, DC power, component cooling, or core heat removal. Fault tree analyses were performed on these systems and point estimates of system unavailabilities were obtained.

The AC power and DC power systems are essentially redundant two-strain systems. Generally, the A and B trains of these systems provide power to the corresponding trains in the safety systems, i.e., AC power Train A provides power for Train A of the safety systems, while AC power Train B provides power to Train B of the safety systems. AC power is required to run pumps and reconfigure AC operated valves, while DC power is required to reconfigure DC operated valves and actuate circuit breakers. DC power is also required for AC power success when the accident sequence is initiated by loss of offsite power. DC power fault contributions were included in the assessment of AC power unavailability. Component cooling is supplied by one of two cooling water systems (the DHCCCS or the NSCCCS). Both component cooling systems depend on the availability of AC and DC power. When offsite power is available, contributions due to AC power and DC power unavailability were assessed to be negligible. When offsite power is lost, AC power unavailability is a significant contributor to system unavailability primarily because of the probability of diesel failure. In this case, the system dependence on DC power is essentially due to the DC power contribution to AC power unavailability. The unavailability of component cooling contributes to individual safety system train unavailability both with and without offsite power available.

Unavailability point estimates of each train of the supporting systems are included as a module on the appropriate train of the modularized safety system fault tree. The interactions among the supporting systems themselves are represented in the Boolean equations for these systems.

5.1.8 EVALUATION OF SYSTEM UNRELIABILITY DURING RECIRCULATION

Point estimates were obtained for the unreliability of safety systems required to operate during the recirculation phase of post-LOCA accidents. It was necessary to estimate the probability that safety system failure occurs during the recirculation phase, as opposed to the probability that the system enters this phase in a failed state, since the consequences of system failure occurring during recirculation are different than if the failure occurred during injection. System failure during recirculation therefore implies system success during injection (if the system is required during both injection and recirculation).

Figure 5.2 shows a generic modularized fault tree for safety system failure during recirculation. System failure could occur during recirculation due to single hardware failures, operator faults that fail the system and are not recovered, or combinations of individual train failures during injection and recirculation.

Referring to Figure 5-2, single hardware faults that occur during recirculation were generally found to be negligible contributors to the probability of safety system failure. Operator faults that could occur during recirculation were evaluated, and for some systems these faults were the dominant contributors to system failure. The assessment of these faults was performed in essentially the same manner as the assessment of operator errors previously described for the injection phase.

Individual train failure during recirculation proncipally involves the failure of operating equipment. Following WASH-1400 assumptions, an operating time period of 24 hours was assumed in all cases. Thus, failure probabilities for operating equipment were computed based on an operating time of 24 hours. As in WASH-1400, it was assumed that recovery from failures after this time would be likely, particularly in view of the fact that equipment requirements diminish with time.

Single train faults during injection were partitioned into two types; those for which no credit was given for recovery by the time the recirculation

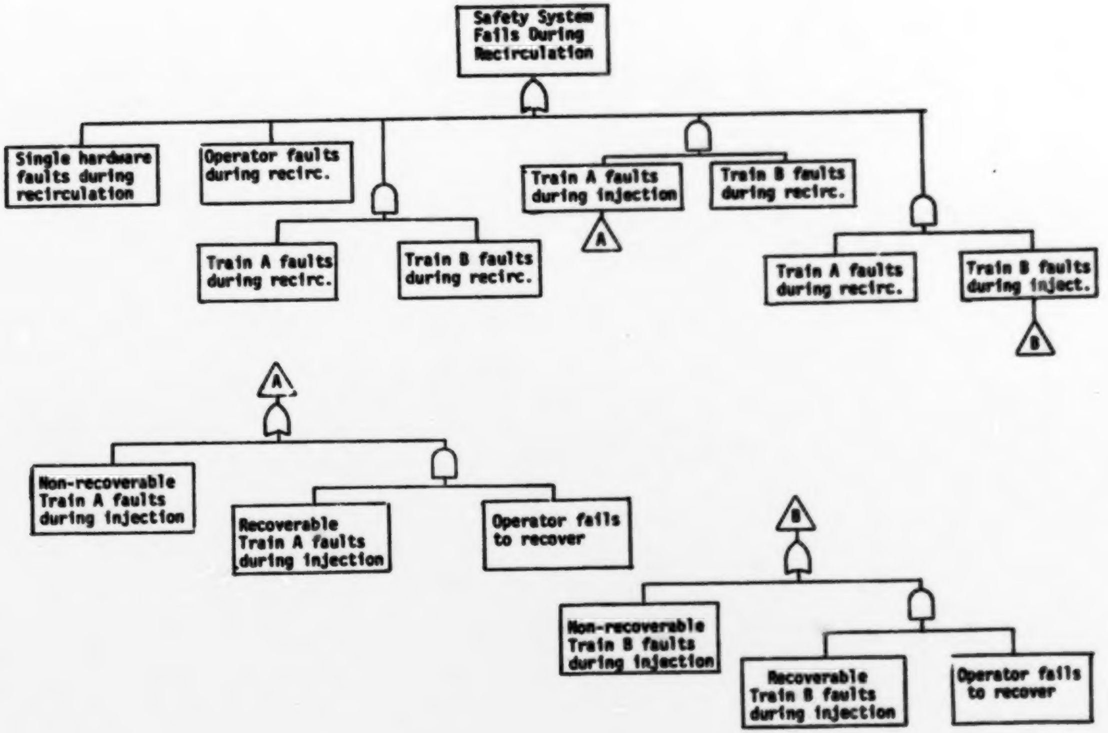

Safety System Fails During Recirculation
Single hardware faults during recirculation
Operator faults during recirc.
Train A faults during injection
Train B faults during recirc.
A
Train A faults during recirc.
Train B faults during recirc.
Train A faults during recirc.
Train B faults during inject.
B
A
Non-recoverable Train A faults during injection
Recoverable Train A faults during injection
Operator fails to recover
B
Non-recoverable Train B faults during injection
Recoverable Train B faults during injection
Operator fails to recover

Figure 5.2 Generic Modularized Fault Tree for "Safety System Fails During Recirculation"

phase began, and those for which recovery was assumed likely. The latter category was comprised of component failures such as fuse failure, human errors that involved leaving valves in incorrect positions, and test outages. No credit was given for starting pumps that failed to start or for reconfiguring motor-operated valves that failed to change state. In all cases, an operator error of failing to recover recoverable faults was assessed; the probability was generally assumed to be 0.1. Interfacing system faults and maintenance outages were assumed to be non-recoverable, except that evaluation of all accident sequences initiated by loss of offsite power assumed that offsite power is restored by the time the recirculation phase begins. (The duration of the injection phase in this case is about 10 hours.) Therefore, a train which fails in injection because a diesel fails would become available again during recirculation. This modeling assumption is reflected in the quantitative analysis.

5.2 FAULT TREE ORGANIZATION AND STRUCTURE

The thrust of the Crystal River study was toward the quantitative evaluation of complete accident sequences as delineated by event trees rather than on obtaining probabilities of system and subsystem failure. Fault trees were treated merely as one link in the chain of analytical elements that constitute sequence evaluations. Although estimates of many of the system failure probabilities were obtained, they are of passing interest only.

Fault tree quantification required two major areas of activity. The first involved organizing the logical structure of the simplified trees so as to reflect the variations in success requirements among different initiating events while taking maximum advantage of the commonality among related fault trees. This process was essential because fault tree development preceded detailed sequence analysis. The other activity involved quantifying individual component-level (primary) faults and combining them to obtain probabilities of higher-level but independent events. The latter are represented by fault tree "modules," i.e., independent subtrees. The actual quantification of the primary events and independent modules followed the methods and assumptions outlined in Section 5.1. The present section concentrates on the logical structure of the fault trees and their equivalent Boolean equations. The presentation of primary faults and fault tree modules is discussed briefly, although the analysis and most of the results are contained in appendices.

5.2.1 A Fault Tree Hierarchy

The starting point for fault tree evaluation was the set of simplified fault trees in which the gate structure was organized according to types of faults (e.g., hardware, operator, outage, etc.). Looking ahead to accident sequence evaluation, and also to the evaluation of recirculation phase faults in the case of LOCAs, it was necessary to impose a greater degree of organizational structure onto the fault trees; it was found that four levels of events were adequate and convenient. Thus, Boolean variables were defined to represent the various systems at four levels of detail. A Boolean equation and the fault tree (or sub-fault tree) it represents are entirely equivalent and therefore interchangeable; Boolean equations were used exclusively for analysis, although fault trees are often retained for display. The four levels of detail are described below:

1. Functional-Level Faults. These are generic faults used in event tree development; they are also sometimes used directly as event tree headings. An example of such a fault is failure of emergency coolant injection, given a LOCA, with Boolean symbol ECI. The functional-level variables are input variables for the equations representing accident sequences through the core-melt stage. In turn, they are represented by equations with input variables from lower levels of faults, but primarily from the second level. Probabilities of the functional level faults were not calculated explicitly for Crystal River.

Some of the functional level faults are discussed more fully in Section 5.2.3 below.

2. System-Level Faults. These faults are inputs to functional-level faults. The corresponding variables represent system-level failures and therefore constitute the "top events" for system fault trees. An example is failure of high pressure coolant injection (a contributor to ECI failure), given a small-small LOCA; the Boolean variable is HPI. The principal input variables are from the next two levels in the fault hierarchy.

Sometimes, event tree headings are given directly in terms of system-level faults rather than functional faults. For example, in the Crystal River LOCA event trees, some of the headings are defined in terms of the Reactor Building Spray System and the Reactor Building Emergency Cooling System rather than in terms of the respective functions they perform, namely Post Accident Radioactivity Removal and Containment Overpressure Protection.

The equations representing first and second level faults are derived from the functional and system success requirements as shown in Tables 4.3 and 4.6.

3. Subsystem (train) -Level Faults. These faults are comprised of the failures of independent trains within redundant systems. They contribute to the system-level faults and are represented by high-level subtrees in the system fault trees. They occasionally contribute directly to functional-level faults. Subsystem-level faults in coolant injection phase functions (in the event of a LOCA) also appear in the equations or fault trees representing recirculation phase functions. This is the main reason that distinct Boolean variables are defined at this level.

4. Fault Tree Modules. These are intermediate events whose inputs are generally at the component level. They can contribute directly at any of the three higher levels in the fault hierarchy. The contributing faults in a given module do not appear elsewhere in any fault tree (although a given module may appear in more than one place) and their probabilities are independent of those of all other faults. Hence, the modules are independent subtrees (most often a simple OR gate). Their use greatly reduces the necessary number of explicit variables and so facilitates manipulation and reduction of the Boolean equations. In general, separate modules are defined for different types of faults so as to maintain some semblance of the organization of the original simplified fault trees.

The hierarchy outlined above was formulated expressly for the Crystal River study as a matter of convenience and in the interests of traceability and scrutability. It is not absolutely essential to the basic approach and is not used in a rigid manner, i.e., exceptions (usually self-evident) are allowed when it is convenient to allow them.

5.2.2 System and Subsystem-Level Faults

System-level faults were derived from the functional and system success requirements outlined in Section 4 for the transient and LOCA event trees. These were the "top events" from which the fault trees were originally developed. The subsystem or train-level faults are subtrees in the system fault trees. They are usually assigned Boolean variables to maintain visibility of system redundancy and because they often appear in more than one system-level fault tree.

Variables representing the system and subsystem-level faults appearing in LOCA sequences are identified with the appropriate initiators and systems in Table 5.3; the actual definitions of the variables are provided in Table 5.4. The latter table also gives the "point estimate" conditional probabilities (with the initiating event given). Note that the probabilities of some faults vary among initiating events. These results are not used explicitly but are included for the benefit of those interested in quantitative analysis at the system level of detail.

Similar information is provided for the transient sequences in Tables 5.5 and 5.6, except that for transients which progress to LOCAs, the LOCA segment of the sequences are characterized by the entries for a B4 LOCA in Tables 5.3 and 5.4.

A separate Boolean equation (or fault tree) is required for each of the variables identified in the tables, but there is a great deal of interdependence and commonality among them. The fault trees and corresponding Boolean equations are given for all system-level and most subsystem-level faults in the appendices. The modular faults which enter into these equations are defined in tabular form as discussed later in Section 5.2.4.

With the exception of the Nuclear Services Closed Cycle Cooling System (NSCCCS), which is a single train system, system-level faults are not defined for the support systems. Only the train-level faults are required for the sequence evaluations.

It may be noted that for the Reactor Building Spray System, the Reactor Building Emergency Cooling System and for the support systems, the same variables (i.e., fault trees) are used for both transients and LOCAs. For transients which do not progress to LOCAs, however, the union of the injection and recirculation phase faults are used. This simply means the system can fail "early OR late," there being no actual distinction between injection and recirculation for such sequences. The total period used in the evaluation was 24 hours.

Table 5.3. Identification of System and Subsystem-Level Events Contributing to LOCA Event Tree Functions[1]

INITIATING LOCA	HIGH PRESSURE COOLING SYSTEM	LOW PRESSURE COOLING SYSTEM	CORE FLOOD SYSTEM	REACTOR BUILDING EMERGENCY COOLING SYSTEM	REACTOR BUILDING SPRAY SYSTEM	SUPPORT SYSTEMS	ENGINEERED SAFEGUARDS ACTUATION SYSTEM
B1	None	Injection: LPI - - - - - - - LA LB LPA LPB Recirculation: LPR LRR - - - - - - - LIR LRI	CFS - - -	Injection: FCI - - - - - - - - Recirculation: FCR - - - - - - - - -	Injection: CSI1 - - - - - - - - - CSA* CSB* Recirculation: CSR - - - - - - - - CSA** CSB** CRA CRB	Injection: N DA DB ACA ACB DCA DCB Recirculation: N* DA* DB* ACA* ACB* DCA* DCB*	ILB1 ILB2 ILB3 ILB4 ILB5 ILS
B2							
B3	Injection: HPI - - - - - - - - - -		None		Injection: CSI3 CSA CSB Recirculation: CSR - - - - - - - - CSA** CSB** CRA CRB		
B4 (including transient-induced LOCA)	Injection: HPI - - - - - - - - - - HA HB Recirculation: HPR - - - - - - - - - - HA* HB*	Recirculation: LHR - - - - - - - - LHA LHB					ISS1 ISS2 ISB

1. Dashed lines separate system-and subsystem-level faults.

BEST DOCUMENT AVAILABLE

Table 5.4. Definitions of System and Subsystem-Level Boolean Variables Used in LOCA Sequence Analysis (Listed by systems; see notes at bottom of table.)

		Estimated Probability
High Pressure Cooling System		
HPI	High pressure injection system fails to provide one pump flow via two injection lines to cold legs; given B3, B4 or transient induced LOCA	(S) 5.7E-2 (L) 5.8E-2 (NL) 5.4E-2
HA (HB)	High pressure injection system Train A fails to provide one pump flow to injection line headers; given B4 or transient-induced LOCA	(S,NL) 1.6E-3 (L) 5.1E-3
HPR	High pressure system fails to provide at least one pump flow via two injection lines to cold legs in the recirculation phase, given HPI succeeds and the corresponding low pressure trains provide adequate suction head to the high pressure pumps; given B4 or transient-induced LOCA	(S) 8.4E-2 (L) 8.3E-2 (NL) 8.3E-2
HA* (HB*)	High pressure system Train A fails to provide at least one pump flow to injection line headers during recirculation, given success during injection and adequate suction head from the corresponding low pressure pump; given B4 or transient-induced LOCA	8.0E-3(2.8E-2)
Low Pressure Cooling System		
LPI	Failure of Low Pressure System to provide at least one pump flow to reactor vessel during injection; given B1, B2 or B3 LOCA.	1.0E-1
LA (LB)	Low Pressure Train A failures from BWST to crossover during injection; given B1, B2 or B3 LOCA.	1.9E-2
LPA (LPB)	Failure of low pressure Train A to provide flow to reactor vessel during injection; given B1, B2 or B3 LOCA.	2.0E-2
LPR	Failure of low pressure system to provide at least one pump flow to reactor vessel during recirculation; given B1, B2 or B3 LOCA.	4.1E-3
LRR	Failure of both low pressure system trains to provide flow to the reactor vessel during recirculation; given B1, B2 or B3 LOCA.	1.2E-5
LIR	Failure of low pressure system Train A during injection and of Train B during recirculation to provide flow to reactor vessel; given B1, B2 or B3 LOCA.	3.8E-5
Low Pressure Cooling System (Continued)		
LRI	Failure of low pressure system Train B during injection and of Train A during recirculation to provide flow to reactor vessel; given B1, B2 or B3 LOCA	3.8E-5
LHR	Failure of low pressure system to provide flow to suction of at least one high pressure train during recirculation; given B4 or transient-induced LOCA	5.4E-2
LHA (LHB)	Failure of low pressure system to provide flow to suction of high pressure Train A during recirculation; given B4 or transient-induced LOCA	5.5E-2
Core Flood System		
CFS	Failure of either core flood tank to deliver contents to reactor vessel at 600 psi; given B1 or B2 LOCA	8.4E-4
Reactor Building Emergency Cooling System		
FCI	Failure of fan cooler system to provide at least 1/3 fan cooling to containment during injection phase; given a LOCA	(L) 3.5E-3 (S,NL) 2.7E-3
FCR	Failure of fan cooler system to provide at least 1/3 fan cooling to containment during recirculation phase; given a LOCA	2.5E-4
Reactor Building Spray System		
CSI1	Failure of both containment spray trains to provide containment atmosphere cooling during injection; given B1 or B2 LOCA	5.1E-2
CSA* (CSB*)	Failure of containment spray Train A to provide containment atmosphere cooling during injection; given B1 or B2 LOCA.	1.2E-2
CSI3	Failure of both containment spray trains to provide containment atmosphere cooling during injection; given B3, B4 or transient-induced LOCA	6.1E-2

Notes:
1. Train B variables shown in parentheses are analogous to the corresponding Train A variables. If the probabilities are different, the Train B probability is shown in parentheses.
2. Individual train variables do not include single or common mode faults that would fail both trains.
3. Recirculation failures imply success during injection (see text for exceptions with loss of offsite power).
4. The evaluation period is 24 hours for injection and recirculation combined.
5. Probabilities preceded by labels apply only to specific initiating events, as follows: S, spontaneous LOCA; L, Loss-of-offsite-power transient-induced LOCA; NL, non-LOSP transient-induced LOCA.

Table 5.4. Definitions of System and Subsystem-Level Boolean Variables Used in LOCA Sequence Analysis (Listed by systems; see notes at bottom of table.) (Continued)

		Estimated Probability
Reactor Building Spray System (continued)		
CSA (CSB)	Failure of containment spray Train A to provide containment atmosphere cooling during injection; given B3, B4 or transient-induced LOCA	1.2E-2
CSR	Failure of both containment spray trains to provide containment atmosphere cooling during recirculation; given LOCA	4.0E-3
CSA**(CSB**)	Failure of containment spray Train A to provide containment atmosphere cooling during injection, due to non-recoverable faults; given LOCA	1.1E-2
CRA (CRB)	Failure of containment spray Train A to provide containment atmosphere cooling during recirculation; given LOCA	4.4E-3
Nuclear Services Closed Cycle Cooling System		
N	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for component cooling during injection; given LOCA	(S,NL) 1.3E-4 (L) 2.8E-3
N*	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal for cooling during recirculation; given LOCA	1.0E-5
Decay Heat Closed Cycle Cooling System		
DA (DB)	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during injection; given demand.	(S,NL) 5.8E-3 (L) 3.8E-2
DA* (DB*)	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling or decay heat removal during recirculation; given demand	1.7E-3
Emergency AC Power		
ACA (ACB)	No power on 4160 V ESF bus 3A during injection; given a LOCA	(S,NL) ε (L) 3.2E-2
ACA* (ACB*)	No power on 4160 V ESF bus 3A during recirculation; given a LOCA	ε
Emergency DC Power		
DCA (DCB)	Insufficient power on DC Train A buses during injection; given a LOCA.	(S,NL) ε (L) 3.2E-3
DCA* (DCB*)	Insufficient power on DC Train A buses during recirculation; given a LOCA.	ε
Engineered Safeguards Actuation System		
ISS1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment; given B4 LOCA	2.1E-4
ISS2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment; given B4 LOCA	2.2E-4
ISB	HPI actuation signal not available to any equipment; given B4 LOCA	7.2E-4
ILB1	Non-time delayed HPI actuation signal not available to exactly 1 piece of equipment; given B1, B2 or B3 LOCA	1.0E-7
ILB2	Time delayed HPI actuation signal not available to exactly 1 piece of equipment; given B1, B2 or B3 LOCA	5.6E-6
ILB3	LPI actuation signal not available to exactly 1 piece of equipment; given B1, B2 or B3 LOCA	1.0E-7
ILB4	RBIC actuation signal not available to exactly 1 piece of equipment; given B1, B2 or B3 LOCA	1.3E-6
ILB5	Containment spray equipment does not receive actuation signal; given B1, B2 or B3 LOCA	1.2E-6
ILS	All RBIC and RBSS equipment does not receive actuation signal; given B1, B2 or B3 LOCA.	1.1E-4

Notes:
1. Train B variables shown in parentheses are analogous to the corresponding Train A variables. If the probabilities are different, the Train B probability is shown in parentheses.
2. Individual train variables do not include single or common mode faults that would fail both trains.
3. Recirculation failures imply success during injection (see text for exceptions with loss of offsite power).
4. The evaluation period is 24 hours for injection and recirculation combined.
5. Probabilities preceded by labels apply only to specific initiating events, as follows: S, spontaneous LOCA; L, Loss-of-offsite-power transient-induced LOCA: NL, non-LOSP transient-induced LOCA.

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table 5.5. Identification of System and Subsystem-Level Events Contributing to Transient Event Tree Functions[1]

INITIATOR[2]	EMERGENCY FEEDWATER SYSTEM	PRIMARY MAKEUP	CONTAINMENT PRESSURE REDUCTION	POST-ACCIDENT RADIOACTIVITY REMOVAL	SUPPORT SYSTEMS[3]
TRANSIENTS WITHOUT LOSS OF NORMAL FEEDWATER: T_1-T_{1A}, T_{1A}	EF1		FCI + FCR CSI1 + CSR	CSI1 + CSR	N + N* DA + DA* DB + DB* ACA + ACA* ACB + ACB* DCA + DCA* DCB + DCB*
TRANSIENTS WITH LOSS OF NORMAL FEEDWATER: T_2-T_{2A}		With loss of all secondary cooling: HPFB - - - - - - - - - - - - HAF HBF			
LOSS OF OFFSITE POWER: T_{2A}	EF2				

Notes: 1. Dashed line separates system-and subsystem-level faults.

2. For the LOCA segment of transient-induced LOCA sequences, see the table of Top Events for LOCA Event Trees.

3. N + N* means N OR N*, etc.

Table 5.6. Definitions of System and Subsystem-Level Boolean Variables Used in Transient Sequence Analysis (Listed by system or function; see notes at bottom of table.)

		Estimated Probability
Emergency Feedwater System		
EF1	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 once-through steam generators, given offsite power is available.	3.4E-4
EF2	Failure of EFS to provide at least 1/2 pump flow to at least 1/2 once-through steam generators, given a loss-of-offsite power transient.	1.8E-3
Primary Makeup (High Pressure Cooling System)		
HPFB	Operator fails to establish feed and bleed operation or high pressure injection system fails to provide one pump flow via two injection lines to cold legs; given transient with loss of all secondary cooling.	(L)1.9E-3 (NL)1.4E-2
HAF (HBF)	High pressure injection Train A fails to provide one pump flow to injection line headers for feed and bleed; given transient with loss of all secondary cooling.	(L)5.0E-2(6.0E-2) (NL)1.4E-3(2.8E-2)
Containment Pressure Reduction		
FCI + FCR	Failure of Reactor Building Emergency Cooling System to provide at least 1/3 fans to cool containment for 24 hours, given demand	(L)3.8E-3 (NL)3.0E-3
CSI1 + CSR	Failure of both containment spray trains to provide containment atmosphere cooling for 24 hours, given demand.	5.5E-2
Post-Accident Radioactivity Removal		
CSI1 + CSR	See above.	5.5E-2
Nuclear Services Closed Cycle Cooling System		
N + N*	Failure of the NSCCCS to deliver one pump flow with ultimate heat removal, given demand.	(L)2.8E-3 (NL)1.4E-4
Decay Heat Closed Cycle Cooling System		
DA + DA* (DB + DB*)	Failure of DHCCCS Train A to provide one pump flow with ultimate heat removal for component cooling and decay heat removal.	(L)4.0E-2 (NL)7.5E-3
Emergency AC Power		
ACA + ACA* (ACB + ACB*)	No power on 4160 V ESF bus 3A, given demand.	(L)3.2E-2 (NL) ε
Emergency DC Power		
DCA + DCA* (DCB + DCB*)	Insufficient power on DC Train A buses, given demand.	(L)3.2E-3 (NL) ε

Notes:
1. Evaluation period is 24 hours.
2. LOCA segments of transient-induced LOCAs are treated with the LOCA sequences.
3. Train B variables shown in parentheses are analogous to corresponding Train A variables. If the probabilities are different, the Train B probabilities are shown in parentheses.
4. Individual train variables do not include single or common mode faults that would fail both trains.
5. Probabilities preceded by labels apply only to specific transients (excluding LOCAs), as follows: L, LOSP transients; NL, non-LOSP transients.

BEST DOCUMENT AVAILABLE

As indicated in the notes to Table 5.4, recirculation failures following a LOCA imply success during injection. There are exceptions to this, however, when the initiator is Loss-of-Offsite-Power (LOSP). It is assumed that if an LOSP transient progresses to a LOCA, the offsite power is restored by the time the cooling systems are switched to the recirculation mode (typically about 10 hours). This means a single train of a cooling system could fail in recirculation even if it had failed earlier, provided the earlier failure was due to failure of the appropriate diesel generator to start. Thus, when train-level injection faults (such as HA, LHA, etc.) appear in equations for recirculation faults (such as HPR), there is implied in their definitions that the injection failures are due to faults other than failure of diesels to start, i.e., due to non-recoverable faults. Although different symbols are not used for the injection faults in these cases, they are noted as they occur throughout the appendices and the appropriate numerical adjustments are made in the calculations. Of course, if, given an LOSP-induced LOCA, both diesels fail to start, the coolant injection function is deemed to have failed, so success or failure of emergency coolant recirculation becomes moot.

For single train faults in general (e.g., HA, HA*, LPA) the respective Boolean equations or fault trees do not include single or coupled failure modes common to both trains in the system. This practice was adopted as a matter of convenience in Boolean reductions; it is not indicated explicitly in variable definitions but is noted in the appendices. The system-level events of course do include the singles and common modes.

In the case of the Engineered Safeguards Actuation System, it was not necessary to define an actuation fault for every piece of equipment supposed to receive a signal. Generic faults, such as "...signal not available to exactly one piece of equipment" were generally adequate.

Fault trees were constructed and evaluated for two systems which are not cited in the tables. The Reactor Protection System (RPS) is essentially independent of the other systems, so there was no need to treat the fault hierarchy explicitly. The failure probability simply enters as a multiplicative factor in the evaluation of the accident sequences. The Containment Isolation System (CIS and CIS*) was evaluated for its contribution to containment leakage probability. It enters into the containment event tree as a contribution to the failure mode β rather than into the system response event trees.

5.2.3 Functional Level Faults

Event tree headings which are defined in terms of functional faults involving more than one system include Emergency Coolant Injection (ECI) and Emergency Coolant Recirculation (ECR) in the LOCA event trees and Containment Pressure Reduction in the transient trees. Other headings were defined directly in terms of system failures appearing among those presented earlier.

Having defined the system-level variables, the functional faults can now be presented in terms of specific system faults. For ECI and ECR, the appropriate expressions, derived from the success requirements, are presented in Table 5.7. (It may be of interest to note that the actual analysis proceeds in the reverse direction, i.e., functional faults are first defined in the process of event tree construction and subsequently translated into system failures.)

Table 5.7. Boolean Expressions for ECI and ECR

Initiator	ECI	ECR
B1	LPI + CFS	LPR
B2	LPI + CFS•(LPA + LPB)	LPR
B3	HPI + LPI	LPR
B4	HPI	HPR + LPR + HA*•LHB + HB*•LHA

Note: "+" ≡ OR; "•" ≡ AND.

In the recirculation phase, the expressions in Table 5.7do not give credit for reactor water cooling by the fans (Reactor Building Emergency Cooling System) when one of the main heat removal systems (DHCCCS or NSCCCS) fails. This may be slightly conservative but it is of very little quantitative significance.

For a small-small (B4) LOCA, the equation ECI = HPI assumes the reactor is shutdown. If this is not the case (i.e., if reactor scram fails), ECI success requires 2 of 2 rather than 1 of 2 trains of the high-pressure system and also 1 of 2 trains of the emergency feedwater system. The probability of ECI failure would be slightly higher in this case but the low probability of scram failure removes such sequences from the realm of major interest in the present study. These and other anticipated transients without scram (ATWS) are discussed in Section 5.3.4.

In the recirculation phase of a B4 LOCA, the Boolean expression for ECR reflects the requirement that successful low and high pressure trains must be aligned to each other to achieve success. (The low pressure pumps boost the suction head to the high pressure pumps.) The expressions for LHA and LHB (presented in Appendix K) reflect also the possibility that in the event of some low-pressure system faults, cross-over valves can be opened to re-align a low-pressure train with the opposite high-pressure train. On the other hand, although both are required, alignment of low and high pressure systems is not necessary for ECI success in the event of a B3 LOCA.

The Containment Pressure Reduction (CPR) function, in the event of a non-LOCA transient, can be performed by either the Reactor Building Spray System (sprays) or the Reactor Building Emergency Cooling System (fans); hence, both systems must fail for the function itself to fail. This is true also for LOCAs, but in the LOCA trees, separate headings are already used for the two systems rather than a single heading for the function. For the transient case, therefore, letting the symbol CPR represent failure of CPR upon demand, we have

$$\mathrm{CPR} = (\mathrm{CSI1} + \mathrm{CSR})\cdot(\mathrm{FCI} + \mathrm{FCR})$$

where again the union of LOCA injection and recirculation variables is used for the 24-hour operating interval.

The Post Accident Radioactivity Removal (PARR) function is also performed by the spray system; hence the last two events in the transient sequences are not independent even at the system level. After system-level Boolean reductions are performed, the last two events in the non-LOCA transient sequences of primary interest (T8, T9, T10) can be represented by the following:

$$\begin{aligned}
\mathrm{T8:}\quad & \overline{0}\cdot\overline{0}' = \overline{\mathrm{CPR}}\cdot\overline{\mathrm{PARR}} = \overline{\mathrm{RBS}} \\
\mathrm{T9:}\quad & \overline{0}\cdot 0' = \overline{\mathrm{CPR}}\cdot\mathrm{PARR} = \mathrm{RBS}\cdot\overline{\mathrm{RBECS}} \\
\mathrm{T10:}\quad & 0 = \mathrm{CPR} = \mathrm{RBS}\cdot\mathrm{RBECS}
\end{aligned}$$

where RBS = CSI1 + CSR, RBECS = FCI + FCR, and a bar over a symbol means success (complement of failure).

Almost all of the system level faults appearing in the Boolean expressions presented are interdependent to varying degrees because of common actuation and support systems, and sometimes because of common or related operator actions. Consequently, all of these expressions require further reduction upon substitution of system fault trees. These reductions are carried out in the course of sequence analysis as described later in Section 5.3.

5.2.4 Fault Tree Quantification Tables

The fault tree modules described earlier are the lowest level events in the fault hierarchy to appear explicitly in the system Boolean equations. They therefore play the role of basic or primary events from the viewpoint of sequence analysis, even though they actually represent intermediate events in the system fault trees. The definition, quantification, and documentation of fault tree modules are contained in fault tree quantification tables which appear in the appendices on individual systems. The purpose here is simply to illustrate the modular technique by presenting some examples from the high pressure cooling system analysis.

The Boolean equations themselves serve as guides to the fault tree quantification tables. The equations for High Pressure Injection (from Appendix G) are shown for illustration in Table 5.8. The top events HPI, HA and HB were defined earlier in Table 5.4. Some of the symbols on the right hand side of the equations represent subsystem-level events (in this case, HA and HB) as defined earlier, and some represent intermediate events which are defined in the table immediately below the top event equations. Symbols not falling into one of these two categories may be identified as fault tree modules whose definitions are to be found in the fault tree quantification tables. The Boolean equations and the quantification tables in combination provide the basic documentation of the fault tree analysis. Modularized system and subsystem fault trees are used as an alternative or supplementary means of presentation in the fault tree appendices.

The equations based on the fault trees are generally not in reduced form; this is intentional, the purpose being to retain visibility of the basic structure of high-level fault trees. The equations for intermediate events are often also not reduced. In this case, for example, HX1 and HX2 represent interfacing system faults; the equations are written so as to retain visibility of these faults. If the appropriate system fault trees (for AC power, DC power, and NSCCCS) were inspected, it would be seen that N contains ACA which in turn contains DCA, so the reduced form of HX1 would simply be HX1 = N; similarly HX2 = DB.

Table 5.8 Boolean Equations for High Pressure Injection

BOOLEAN EQUATIONS BASED ON MODULARIZED FAULT TREES

Top Events

$$HPI = HA \cdot HB + H1 \cdot H2 \cdot (H3 \cdot H4) + H5 + H6 + H7 + H9 + L3 + $$
$$+ L017 + H01 + (H02 \cdot H8) \cdot LOCA + (H04 \cdot ACA) \cdot AL$$

$$HA = HX1 + H10 + H11 \cdot H12 + H13 + H1 \cdot (AL + H2) \cdot (H3 + H12 + H17 + H14)$$

$$HB = HX2 + H4 + H15 + H16 + H18$$

Intermediate Events

$$HX1 = ACA + DCA + N \quad (=N)$$
$$HX2 = ACB + DCB + DB \quad (=DB)$$
$$HX1 \cdot HX2 = ACA \cdot ACB + ACA \cdot (D2 + D4 + DM2 + DH2) + DB[N1 + N2\ (N3 + NM2) +$$
$$+ N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 +$$
$$+ N3 \cdot NM1]$$

BOOLEAN EQUATIONS REGROUPED FOR REDUCTION

Top Event

$$HPI = H5 + H6 + H7 + H9 + L3 + L017 + H01 + H02 \cdot H8 \cdot LOCA + (H04 \cdot ACA) \cdot AL +$$
$$+ HX1 \cdot (H4 + H15 + H16 + H18) + ACA \cdot ACB +$$
$$+ HX2 \cdot \{H10 + H11 \cdot H12 + H13 + H1 \cdot [AL \cdot (H3 + H12 + H17 + H14) +$$
$$+ H2 \cdot (H12 + H17 + H14) + H2 \cdot H3]\} + (H10 + H11 \cdot H12 + H13) \cdot$$
$$\cdot (H4 + H15 + H16 + H18) + H1 \cdot \{(H4 + H15 + H16 + H18) \cdot$$
$$. [AL \cdot (H3 + H12 + H17 + H14) + H2(H12 + H17 + H14)] +$$
$$+ H2 \cdot H3 \cdot (H15 + H16 + H18) + H2 \cdot (H3 \cdot H4)\} +$$
$$+ ACA \cdot (D2 + D4 + DM2 + DH2) + DB\ [N1 + N2 \cdot (N3 + NM2] +$$
$$+ N6 \cdot (N5 + NM4) + N4 \cdot (N5 + N7 + NM4) + NM3 \cdot (N5 + N7) + N6 \cdot N7 + N3 \cdot NM1]$$

Intersections of events with non-independent probabilities are usually shown in parentheses (e.g., H3•H4); double faults in which one fault is an operator failure to recover from the other fault are often shown in parentheses also (e.g., H02•H8).

When all substitutions are made, the "multiplications" carried out, and the Boolean reductions performed, the fully reduced system top event equation is obtained. This is shown as the last expression in the table. It appears under the heading "Boolean Equations Regrouped for Reduction"; this reflects the fact that, although the equation is itself reduced, when combined with other system equations to form sequence equations, further reduction will be necessary because of system interdependencies.

A segment of the quantification table for events HA, HB, and HPI is shown for illustration in Table 5.9. The EVENT column gives the Boolean symbol for a fault tree module, while the COMPONENT column lists the components whose faults contribute to the module. In most cases, a module represents an OR gate with a number of inputs; the inputs are simply listed (see, for example, the event H16). The third column gives descriptive information while the fourth and fifth columns give the failure rate and duration, respectively. The next column gives the unavailability or probability for the component events and shows the summation (the small probability approximation is nearly always valid) by means of a line and Σ symbol. This is further indication the module represents an OR gate. The total is usually entered also at the top in line with the event symbol, so this value often appears twice. The symbol ε implies a negligible value, usually less than 1.0E-6.

Some event symbols represent conditions (i.e., "houses") so no component is indicated; examples include H1, H11 and AL. Some events, H01 for example, represent a single fault.

Sometimes modules appear in double events. If so, the complete double is shown in the event column (e.g., H8•H02 in Table 5.9) to clearly indicate the intended logic. The inputs are usually listed and quantified separately; the product of probabilities is indicated by the symbol π and again is entered at the top as the probability of the complete event.

For double events comprised of coupled faults, the double may also be shown explicitly in the event column, but the input events are not usually listed since they are similar events. These events are quantified by means

BEST DOCUMENT AVAILABLE

Table 5.9 Segment of Quantification Table for Events HA, HB and HPI

EVENT	COMPONENT	EVENT OR FAULT DESCRIPTION	FAILURE RATE(HR^{-1})	FAULT DURATION(HR)	UNAVAILABILITY OR PROBABILITY	ERROR FACTOR	SENS.	NOTES
H16		TRAIN B PUMP FAULTS			2.0 E-3			
	PUMP MUP-1C	FAILS TO START	D		1.0 E-3	$3^+, 3^-$		
	CIRCUIT BKR.	FAILS TO CLOSE	D		1.0 E-3	$3^+, 3^-$		
					Σ=2.0 E-3			
H1		PUMP 1B RUNNING, PUMP 1A ON STANDBY AT ONSET OF INCIDENT			.75			2
H11		PUMP 1B DOWN, PUMP 1A RUNNING AT ONSET OF INCIDENT			.25			2
AL		INITIATOR IS LOSS OF OFFSITE POWER			1 OR 0			3
H5		PASSIVE SINGLE FAULTS COMMON TO BOTH TRAINS			ε			
L3		BWST NOT VENTED			1.0 E-5			
	2 VACUUM BKRS (DH69 AND 70)	FAIL TO OPEN OR PLUGGED	(1.0E-4)(0.1)		1.0 E-5		B	5
	BWST	RUPTURED			ε			4
	BWST	NOT FULL			ε			4
	PIPE	RUPTURE			ε			4
					Σ= 1.0 E-5			
H8·H02		OPERATOR FAILS TO ISOLATE BREAK IN INJECTION LINE			5.0 E-3	$3^+, 10^-$	0	
H8	INJECTION LINE	BREAK OCCURS IN INJECTION LINE, GIVEN THAT SMALL-SMALL BREAK OCCURS			0.5			6
H02	INJECTION LINE	OPERATOR FAILS TO CLOSE VALVE	D		1.0 E-2	$3^+, 10^-$	0	
					π=5.0 E-3			
H3·H4	MANUAL VALVES 10, 70, 2, 59	2 VALVES LEFT CLOSED IN ANY OF THE COMBINATIONS: 70-59, 2-10, 70-2, 10-59	D		1.0 E-3	$10^+, 10^-$	H	7
LOCA		LOCA GATE						
		LOCA			1			
		NON LOCA			0			
H01	OPERATOR	OPERATOR INCORRECTLY TURNS OFF PUMPS AND FAILS TO RECOVER IN TIME TO MITIGATE INCIDENT	D		1.0 E-3	$10^+, 3^-$	0	8

of a beta factor which is shown either as a multiplier of the basic failure rate in the fourth column or is explained by a note. (See for example the event H3·H4, where the coupling is explained in the indicated note, and the failure of two vacuum breakers contributing to L3[1], both of which appear in Table 5.9). In some cases, the input faults appear separately in the tables as single train faults; this is true of H3 and H4 although they don't appear in the excerpt shown as Table 5.9). The coupled doubles appear explicitly in the Boolean equations and are quantified with the appropriate value from the table, rather than with the product of the independent probabilities.

In those few cases where the module logic is not apparent from the fault listings, an explanation is given in numbered notes which accompany the complete tables; the notes are referenced in the last column. These notes also explain the quantification of individual faults where such explanation is necessary, indicate specific assumptions, and identify exceptions to the general analytical procedures. The notes are an integral part of the documentation.

Sometimes an event or module appears in more than one equation associated with a given system. Since the fault listings are ordered to facilitate following the logic represented by the equations, these events or modules appear more than once in the tables. This repetition is intentional. Again, the equations provide the essential guides to the fault tree logic.

The seventh and eighth columns, labeled ERROR FACTOR and SENS. (for SENSITIVITY), were included in anticipation of future sensitivity studies; the information contained in these columns was not used in the present study. The error factors were taken directly from the failure rate data base (Tables 5.1a and b when given there; otherwise they were simply estimated. Upper and lower bounds of an uncertainty range are obtained, respectively, by multiplying the point unavailability by the factor labeled "+", and by dividing it by the factor labeled "-". This uncertainty range is given no precise statistical significance except that the probability of it containing the actual event probability is believed to be high. The SENSITIVITY column is used simply to identify (by labels) faults in selected categories which are of particular interest from the standpoint of uncertainty and sensitivity. The labels used are B (for beta factor as used in evaluating coupled faults), O (for operator faults), H (for human errors) and M (for maintenance outages). The absence of a label has absolutely no significance other than indicating that a fault does not belong to one of these categories.

---

[1] In the actual table in Appendix G, the sublisting of faults under L3 does not appear explicitly; it is incorporated by reference from the LPI table (Appendix K) via Note 5. The listing for L3 is shown here for illustration.

5.3 SEQUENCE ANALYSIS

This section discusses the accident sequence quantification procedures and the identification of the dominant accident sequences in the transient and LOCA event trees.

The accident sequences, including the initiating events and containment failure modes, were evaluated by multiplying three probabilities:

- The probability of the initiating event
- The conditional probability of the event tree accident sequence, given the initiating event
- The conditional probability of containment failure (several types), given the initating event and accident sequence

The Boolean reduction required to obtain point estimates of the conditional probabilities of the event tree accident sequences, given the initiating event, is discussed in Section 5.3.1. The choice and quantification of the initiating events is discussed in Section 5.3.2. The analysis to assign conditional probabilities of containment failure for each initiating event-accident sequence combination is presented in Section 5.3.3. The results of the accident sequence quantification are discussed in Section 5.3.4; tables are presented that summarize the results and assign each sequence to an accident category.

5.3.1 Boolean Reduction of Event Tree Sequences

Point estimates were obtained for the transient and LOCA event tree accident sequences leading to core melt. The point estimates of sequence probabilities were obtained by Boolean reduction and quantification of each event tree sequence, using the Boolean equations of the modularized fault trees which represent the event tree headings. Both system successes and system failures were explicitly included in the Boolean reduction of each event sequence so that "unallowed" cut sets would be removed from the sequence equation. These "unallowed" cut sets are those that, in addition to failing a system which does fail in the sequence, would also fail a system specified as succeeding in the sequence. If not removed, they would result in an incorrect numerical result for the event sequence. The unallowed cut sets generally included combinations of modules representing failure of supporting systems (e.g., AC power), certain human errors that had the potential of failing more than one system, and modules representing combinations of components that could fail individual trains of more than one system. Dependencies upon the emergency AC power and cooling system are illustrated in Figure 2.3 with a logical representation similar to that of a fault tree.

To illustrate the Boolean reduction procedure and the necessity for it, consider a portion of the LOCA event tree specifying failure of the Reactor Building Emergency Cooling System (fans) during injection (FCI) together with success of the Reactor Building Spray System (sprays) during injection (CSI). The Boolean expressions for FCI and CSI (from Appendices L and M respectively) are:

$$\mathrm{FCI} = \mathrm{F4} + \mathrm{AL}\cdot\mathrm{ACA}\cdot\mathrm{F5} + \mathrm{N}$$

$$\mathrm{CSI} = \mathrm{K1} + (\mathrm{K2} + \mathrm{DA})\cdot(\mathrm{K3} + \mathrm{DB})$$

where K1, K2 and K3 are themselves independent Boolean variables, with modules as inputs, defined for convenience in this example. The support system faults N, DA and DB are represented by expressions (from Appendices E and F) of the form:

$$\mathrm{N} = \mathrm{XN} + \mathrm{YN}\cdot\mathrm{ACA} + \mathrm{ZN}\cdot\mathrm{ACB} + \mathrm{ACA}\cdot\mathrm{ACB}$$

$$\mathrm{DA} = \mathrm{XDA} + \mathrm{ACA}$$

$$\mathrm{DB} = \mathrm{XDB} + \mathrm{ACB}$$

where XN, YN, ZN, XDA and XDB are also independent Boolean variables. The events ACA and ACB represent failures of Train A and Train B, respectively, of emergency AC power. The essence of the reduction problem is to accommodate the fact that ACA and ACB, (in this example), appear simultaneously in a failure and a success. Substituting for DA and DB in CSI and then taking the complement results in:

$$\overline{\mathrm{CSI}} = \overline{\mathrm{K1}}\cdot\overline{\mathrm{K2}}\cdot\overline{\mathrm{XDA}}\cdot\overline{\mathrm{ACA}} + \overline{\mathrm{K1}}\cdot\overline{\mathrm{K3}}\cdot\overline{\mathrm{XDB}}\cdot\overline{\mathrm{ACB}}$$

Substituting for N in FCI and forming the product FCI·$\overline{CSI}$, the simple example sequence, yields the following twelve cut sets:

1. $F4 \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
2. $F4 \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$
3. $XN \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
4. $YN \cdot ACA \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
5. $ZN \cdot ACB \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
6. $ACA \cdot ACB \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
7. $XN \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$
8. $YN \cdot ACA \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$
9. $ZN \cdot ACB \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$
10. $ACA \cdot ACB \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$
11. $AL \cdot ACA \cdot F5 \cdot \overline{KT} \cdot \overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}$
12. $AL \cdot ACA \cdot F5 \cdot \overline{KT} \cdot \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}$

Note that cut sets 4, 6 and 11 contain the event $ACA \cdot \overline{ACA}$ and cut sets 9 and 10 contain the event $ACB \cdot \overline{ACB}$. These are null events since they each represent simultaneous success and failure of an AC power train, clearly an impossible situation. The seven remaining cut sets can be recombined to obtain the following equation:

$$\begin{aligned} FCI \cdot \overline{CSI} = {} & (F4 + XN) \cdot (\overline{K2} \cdot \overline{XDA} \cdot \overline{ACA} + \overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}) + \\ & + ZN \cdot ACB \cdot (\overline{K2} \cdot \overline{XDA} \cdot \overline{ACA}) + \\ & + (YN + AL \cdot F5) \cdot ACA \cdot (\overline{K3} \cdot \overline{XDB} \cdot \overline{ACB}) \end{aligned}$$

Since module successes have probabilities very nearly equal to one, the factors in square brackets have little quantitative effect; hence, the above expression can be replaced by a surrogate equation, viz.,

$$FCI \cdot \overline{CSI} = F4 + XN + ZN \cdot ACB + (YN + AL \cdot F5) \cdot ACA$$

The surrogate equation is "approximately equal" to the complete equation in the sense that their probabilities are approximately equal. (Note that the surrogate equation could be obtained directly from the seven cut sets simply omitting the successes and taking the Boolean sum, or union, of what remains. (The process works only after all the null events have been eliminated.)

The key feature in the above process is the elimination of the null sets, i.e., removing the "unallowed" cut sets referred to earlier. The net effect in the example was to eliminate ACA·ACB as a contributor to FCI·$\overline{\text{CSI}}$; in fact, the only difference between FCI and the surrogate expression for FCI·$\overline{\text{CSI}}$ is that the term ACA·ACB is missing from the latter. Dropping the successes after eliminating the null sets is a computational convenience with numerical error well within the range of expected uncertainty.

The example above was deliberately made simple for convenience of presentation. It should be recognized, however, that for actual sequences, all the factors, both failures and successes, must be included before the reduction process is carried out. For systems with extensive interdependencies, as in the case of Crystal River-3, the formal Boolean reduction process is both lengthy and costly, even when performed with the aid of computer codes. (The code WAMCUT (5-2) was used in the present study.) A generally applicable and highly reliable short-cut process would be very useful and is probably feasible but has not yet been developed.

Each of the Crystal River sequences, for transients and LOCAs, was reduced as illustrated in the above example. The resulting surrogate equations were quantified to obtain point estimates of the conditional sequence probabilities, given the initiating events.

5.3.2 Initiating Event Frequencies

The two major classes of initiating events considered in this study are transients and LOCAs. Transients are grouped into two basic types:

- Type T_1 - those which do not directly affect the operability of the power conversion system (PCS), and
- Type T_2 - those which result directly in loss of the PCS.

Each of these is further subdivided into two subtypes, as described in Section 4.1, so that four transient categories are defined. LOCA initiators are also grouped into four categories, by size, based on analyses of ECCS capabilities presented in the Crystal River-3 FSAR (also discussed in Section 4.1).

Transient frequencies were estimated on the basis of data from Reference 5-15 (EPRI NP-801). The estimates were presented earlier in Table 4.1a.

The frequency of LOCA initiators was assessed by comparison of CR-3-assumed LOCA sizes to WASH-1400 LOCA frequency data used for Surry-1. The CR-3 small LOCA size range corresponds roughly to the small-small and small LOCA size range used for Surry. We therefore summed the frequency for the two smallest Surry LOCA categories to obtain a frequency of 1.3 E-3/year for the B4 (smallest) CR-3 LOCA. The occurrence frequency for the other CR-3 LOCA sizes (B1, B2, and B3) were assumed to be 1.0 E-4/year, which corresponds to the large LOCA occurrence frequency for Surry. The B1, B2, and B3 LOCA sizes roughly correspond to the range of the Surry large LOCA. Thus, assigning 1.0 E-4/year to each of the CR-3 LOCA categories results in a conservative assessment of these initiator frequences. The specific definitions and the probabilities of each of the LOCA initiators were presented in Table 4.1b.

5.3.3 Probabilities for Special Events in the Transient Event Tree

Four of the events included in the transient event tree were not evaluated by means of fault tree analysis due to their simplicity, or the availability of actual data, or the existence of a sound basis for engineering judgment. These events are:

- Loss of PCS (event M)
- Pressure relief requirement (event P_1)
- Pressure relief (event P_2)
- Reactor vessel integrity (event Q)

In these cases a point estimate probability was used for the event. The basis for each is described below:

(1) Loss of PCS (Event M)

The probability estimated for event M was 0.1/demand. This is based on information indicating that the PCS will be lost following a transient not directly affecting it on the order of once in ten transients. (The probability of event M is 1.0 for loss of PCS transients.)

(2) Pressure Relief Requirement (Event P_1)

This event was included on the event tree for the purpose of distinguishing between those transients which require pressure relief and those which do not for the specific case of reactor trip followed by loss of normal secondary heat removal and success of emergency secondary heat removal (sequences 2-5 on the transient event tree in Figure 4.2). At the time the transient event tree was developed, there was reason to believe that slight phenomenological differences between plant responses to different transient initiators required this distinction to be made. The evaluation of the sequences which resulted would be accomplished by assigning a value of 0.0 or 1.0 to P_1 depending on the transient initiator. Transients which do not require pressure relief would have P_1 set equal to 1.0 ($\overline{P}_1 = 0.0$). Transients which do require pressure relief would have P_1 set equal to 0.0 ($\overline{P}_1 = 1.0$).

By the time the sequence evaluation began, however, changes made at the plant in response to NRCs post-TMI requirements concerning anticipatory trips and relief valve pressure setpoints made the distinction unnecessary. The post-TMI changes eliminated the requirement for pressure relief for this specific scenario for any transient initiator, thus P_1 will always be equal to 1.0 ($\overline{P}_1 = 0.0$), and this value was used in the sequence evaluation.

It is noted that the net effect of setting the probability of $\overline{P}_1$ equal to zero is that all sequences containing $\overline{P}_1$ will have a zero probability. Thus sequences 2,3 and 4 on the transient event tree in Figure 4.2 essentially cease to exist.

(3) Pressure Relief (Event P_2)

The probability estimated for event P_2 (failure to achieve pressure relief) is negligible. This is based on the following engineering judgments:

- Plant response is not significantly affected by small errors in the lift setpoint of a relief or safety valve; i.e., it is not of paramount importance that these valves lift precisely at their setpoints due to the conservative design of the plant.
- It is considered extremely unlikely that the relief and/or safety valves will fail to lift near their setpoints and thus allow PCS pressure to rise to a value sufficient to cause a rupture in the system[1]. (Note that assuming P_2 has negligible probability makes all sequences containing P_2 have negligible probability).

(4) Reactor Vessel Integrity (Event Q)

The assessed probability of event Q (loss of reactor vessel integrity) is 2.0 E-2/demand. This number is based on the probability for failure of safety valves to reseat after opening of 1.0E-2/demand as shown in Table 5.1a and the presence of two safety valves.

5.3.4 Analysis of ATWS Sequences

The ATWS sequences on the transient event tree were analyzed separately from the other sequences and shown to be relatively insignificant contributors to plant risk based on their relatively low probabilities. These sequences are shown in Figure 4.2 as sequences number 15 through 30. Of the 16 sequences on the tree, 12 result in core melt, two result in transient-initiated LOCAs (with a potential for core melt), and two result in a "safe" outcome (no core melt, but possible core damage). This delineation of ATWS sequences is considered realistic and valid for the purposes of this project; however, we did not intend or expect to resolve the long-standing ATWS issue with our evaluation of the ATWS sequences for this reactor. That goal is outside the scope of this project. We did intend to address these sequences and rationally evaluate the relative contributions to risk posed by them in comparison to the risk posed by non-ATWS sequences initiated by transients and LOCAs. This we have done on the basis of sequence probabilities, utilizing all of the information available to us.

---

[1] These judgments may not apply to one or two of the ATWS sequences on the transient event tree, because of the very rapid pressure spike which is expected to occur in the primary system in those cases. The judgments are believed to be valid for all non-ATWS cases and many of the ATWS sequences as well.

The discussion which follows describes individual sequences and groups of sequences and their probabilities. The discussion progresses, in six steps, through all 16 ATWS sequences. The sequences which do not result in core melt are of no interest: those that result in core melt are shown to be of low enough probability to be eliminated from further analysis for the purposes of this project. This discussion and the supporting reference documents form the basis for our conclusion that the ATWS sequences are not significant contributors to risk at Crystal River-3.

1. Sequence 15 - a non-melt sequence eliminated from further consideration.

The normal heat removal system stays in operation (event $\overline{M}$) and primary system integrity is maintained (event $\overline{Q}$), so that the plant continues to operate as if nothing happened, even though some trip setpoint has been exceeded.

2. Sequence 20 - a non-melt sequence eliminated from further consideration.

The loss of normal heat removal (event M) causes a very high pressure spike, but primary system (RCS) integrity is maintained (event $\overline{Q}$), at perhaps a very low but finite probability. With emergency feedwater (EFS) operating (event $\overline{L}$) and RCS intact, the plant power level will equilibrate at a power level equal to the secondary heat demand created by the EFS, due to the basic reactor physics associated with temperature-dependent reactivity. This results in a stable condition at a low power level, with ample time (on the order of more than 10 hours) to effect an orderly shutdown. This is documented in references 5-16 and 5-17 and corroborated by ATWS work performed at Battelle Columbus Laboratory[1].

---

[1] P. Cybulskis, Battelle Columbus Laboratories, personal communication to P. Amico, SAI, and G. Kolb, SNL, November 1979 (several dates).

3. Sequences 25 through 30

All of these sequences include events TKML. Therefore, any one sequence can have a probability no higher than that of TKML and the sum of the probabilities of these six sequences must equal the probability of TKML (from Boolean algebra and simple statistics). Thus, if the probability of TKML is negligible (defined as less than 1.0E-7 in this evaluation), each one of sequences 25-30 must also have negligible probabilities. Figure 5.3 shows the analysis in the form of a fault tree of TKML for each transient class, with the rates for the events noted in the figure. Since the events on these fault trees are independent, they can be multiplied together (within each tree) to demonstrate that the probability of TKML, and thus the probability of each of sequences 25-30, is negligible for all transient initiators. This entire group of sequences is therefore eliminated from further consideration.

4. Sequences 17 through 19 and 22 through 24

Both sets of these sequences contain event P_2, the failure of S/RVs to open on demand. It is conservatively assumed in all of these sequences that occurrence of event P_2 results in core melt. Since the failure of all S/RVs to pen on demand is evaluated as a very small probability (ε), all sequences containing event P_2 must also have very small probabilities (ε) and they can be eliminated from further consideration.

5. Sequence 16

In this transient-initiated LOCA sequence, the power conversion system remains in operation and a large pressure spike does not occur. It is conservatively assumed, however, that the pressure increases enough to lift the S/RVs (this is actually true only for a small fraction of all transients) and that one fails to close. Because the pressure increase will in all cases be small, the S/RVs will pass only steam, and the usual failure rates apply. Analysis provided by Battelle Columbus Laboratories shows that the coolant loss which occurs if a valve sticks open can be mitigated by 2-out-of-3 (2/3) HPI pumps[1]. A review of the HPI analysis in Appendix G

---

[1] P. Cybulskis, Battelle Columbus Laboratories, personal communication to P. Amico, SAI, and G. Kolb, SNL, November 1979 (several dates)

BEST DOCUMENT AVAILABLE

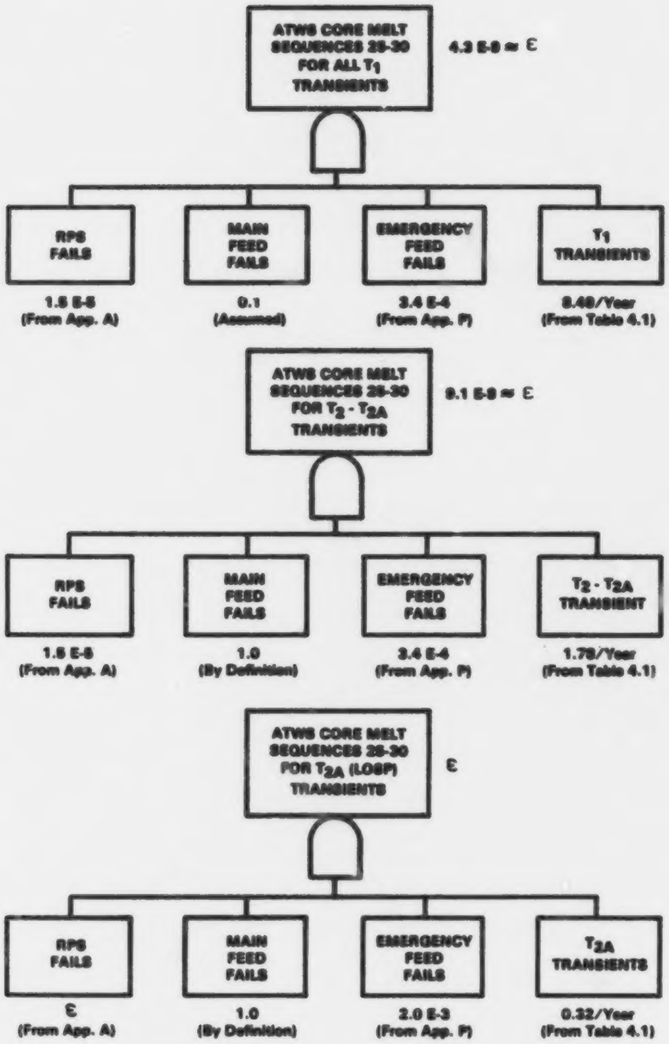

ATWS CORE MELT SEQUENCES 25-30 FOR ALL T_1 TRANSIENTS
4.3 E-9 ≈ ε
RPS FAILS
1.5 E-5 (From App. A)
MAIN FEED FAILS
0.1 (Assumed)
EMERGENCY FEED FAILS
3.4 E-4 (From App. P)
T_1 TRANSIENTS
8.48/Year (From Table 4.1)
ATWS CORE MELT SEQUENCES 25-30 FOR T_2 - T_{2A} TRANSIENTS
9.1 E-9 ≈ ε
RPS FAILS
1.5 E-5 (From App. A)
MAIN FEED FAILS
1.0 (By Definition)
EMERGENCY FEED FAILS
3.4 E-4 (From App. P)
T_2 - T_{2A} TRANSIENT
1.78/Year (From Table 4.1)
ATWS CORE MELT SEQUENCES 25-30 FOR T_{2A} (LOSP) TRANSIENTS
ε
RPS FAILS
ε (From App. A)
MAIN FEED FAILS
1.0 (By Definition)
EMERGENCY FEED FAILS
2.0 E-3 (From App. P)
T_{2A} TRANSIENTS
0.32/Year (From Table 4.1)

FIGURE 5.3. QUANTIFICATION ILLUSTRATIONS FOR ATWS CORE MELT SEQUENCES 25-30 FOR ALL TRANSIENT INITIATORS

shows that the failure of HPI is largely dominated by errors which are independent of the number of pumps required (such as human errors which affect the entire system); thus the failure rate calculated for the system with 1/3 pumps required (1.7E-2) can be applied as an approximation for 2/3 pumps required. The sequence is not analyzed further, since if HPI works, the reaction is shut down, and the sequence behaves exactly like a non-ATWS sequence in recirculation. Figure 5.4 shows tne analysis for this sequence in the form of a fault tree with a probability of 4.3 E=8≈ ε for transient initiators where the PCS remains available (PCS unavailable does not apply), thus eliminating this sequence from further consideration.

6. Sequence 21

This transient initiated-LOCA sequence is similar to sequence 16, described above. The only difference is in the probability of a breach of the primary coolant system because the failure of normal heat removal causes a very high pressure spike of short duration, as described for Sequence 20. Analysis provided by Battelle Columbus Laboratory shows that 2/3 HPI pumps in combination with a successful EFW system can prevent a core melt[1] as in sequence 16. Therefore, the only additional information required is the probability of a loss of RCS integrity. First, the point must be made that there is no reason to believe that a rupture of the vessel itself, causing an uncoolable condition, will occur. Every analysis and indication provided by actual experience has demonstrated that the weakest points in the RCS are the S/RVs and the associated headers and the reactor coolant pump seals and casings. We therefore assume that if the pressure spike causes a breach of the RCS, it will occur in one of these locations[2]. Second, we must determine what estimate to use for a probability of a loss of RCS integrity at one of these locations, given that an overpressure condition has occurred. There is not much data available for this but our experience suggests that less than one-half of the HPI overpressure transients which have occurred have led to a LOCA. We will use 0.5 for the purposes of this

---

[1] P. Cybulskis, Battelle Columbus Laboratories, personal communication to P. Amico, SAI, and G. Kolb, SNL, November 1979 (several dates)

[2] For example, overpressurization of the RCS due to HPI pump start under solid RCS conditions has never led to any breach other than at the S/RVs or the RCS pump seals, if they led to any break at all.

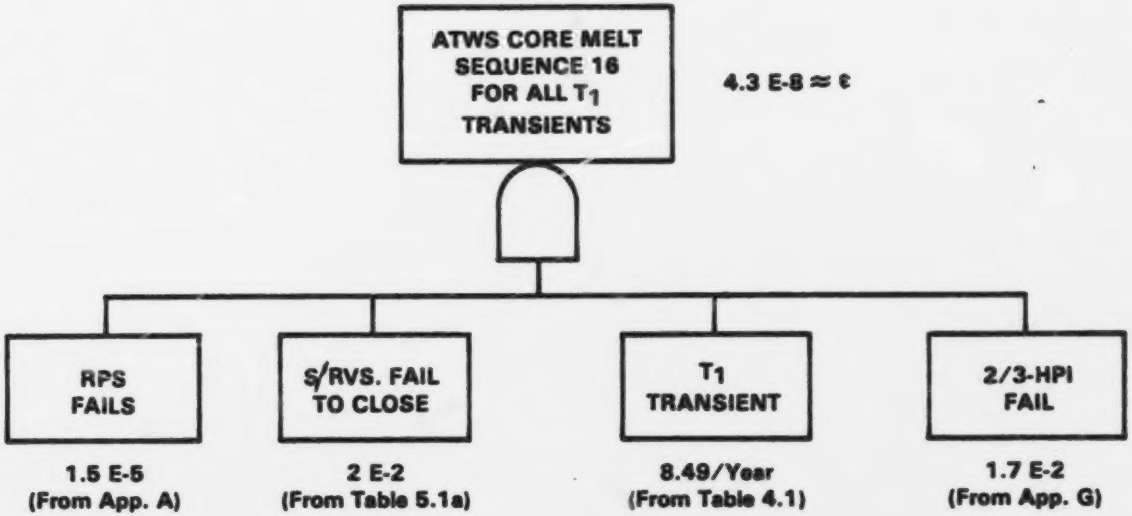

ATWS CORE MELT SEQUENCE 16 FOR ALL T_1 TRANSIENTS
4.3 E-8 ≈ ε
RPS FAILS
1.5 E-5
(From App. A)
S/RVS. FAIL TO CLOSE
2 E-2
(From Table 5.1a)
T_1 TRANSIENT
8.49/Year
(From Table 4.1)
2/3-HPI FAIL
1.7 E-2
(From App. G)

FIGURE 5.4. QUANTIFICATION ILLUSTRATION FOR ATWS CORE MELT SEQUENCE 16 FOR ALL TYPE T_1 TRANSIENT INITIATION

analysis. Figure 5.5 shows a fault tree analysis for this sequence for all transient initiators. The sequence probabilities are not quite negligible, but they are on the order of 1.0E-7. When we also consider the probabilities of the containment failure modes that will be appended to this sequence, those sequences which would be coupled to the α, β and δ containment failure modes (all have probabilities less than 0.1) would become less likely and therefore negligible by the present criterion. Containment failures by hydrogen burning (γ) or by melt-through (ϵ) have probabilities of 0.5 Melt-through for ATWS leads only to release category 7, and, as will be seen, there are already a significant number of accident sequences with probabilities in the order of 1.0E-5 and 1.0E-6 in this category. Hence, no significant contribution would be made by this sequence with containment failure by melt-through. Failure of containment due to hydrogen burning (γ) would lead to releases in category 3, where a similar situation prevails.

5.3.5 Containment Failure Probabilities

The conditional probabilities of the containment failure mechanisms identified in Section 4.5, given an initiating event and accident sequence, were obtained from the Oconee RSSMAP Study (5-18). The five containment failure mechanisms and their possible frequencies are shown in Table 5.10. Not all containment failure mechanisms are possible for every event tree sequence, and the probability of a given containment failure mode is highly initiator and sequence dependent.

Table 5.10 Containment Failure Mode Probabilities

Failure Type	Description	Probability/ Core Melt Event
α	Vessel Steam Explosion	0.01 or 0.0001
β	Containment Leakage	0.007
γ	Hydrogen Combustion	0.2 or 0.5
δ	Overpressure	0.0, 0.5 or 1.0
ε	Melt Through	0.0, 0.5 or 0.8

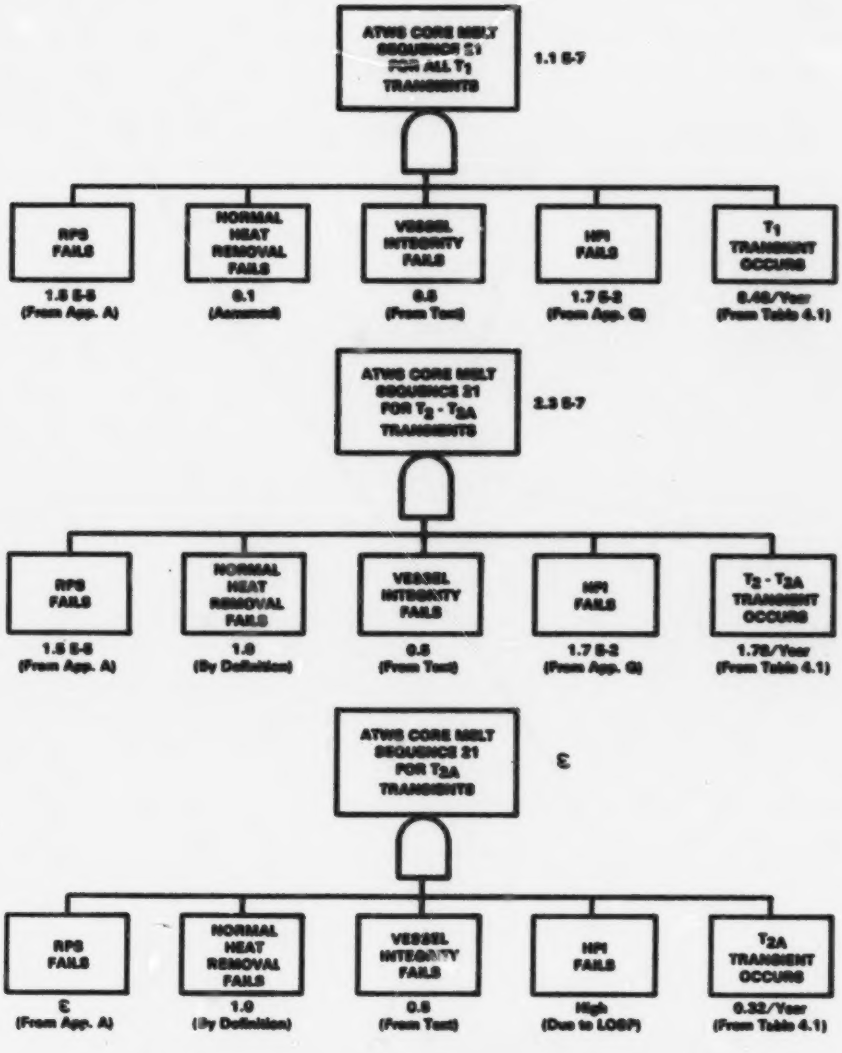

ATWS CORE MELT SEQUENCE 21 FOR ALL T_1 TRANSIENTS
1.1 E-7
RPS FAILS
1.5 E-5
(From App. A)
NORMAL HEAT REMOVAL FAILS
0.1
(Assumed)
VESSEL INTEGRITY FAILS
0.5
(From Text)
HPI FAILS
1.7 E-2
(From App. G)
T_1 TRANSIENT OCCURS
8.48/Year
(From Table 4.1)
ATWS CORE MELT SEQUENCE 21 FOR T_2 - T_{2A} TRANSIENTS
2.3 E-7
RPS FAILS
1.5 E-5
(From App. A)
NORMAL HEAT REMOVAL FAILS
1.0
(By Definition)
VESSEL INTEGRITY FAILS
0.5
(From Text)
HPI FAILS
1.7 E-2
(From App. G)
T_2 - T_{2A} TRANSIENT OCCURS
1.78/Year
(From Table 4.1)
ATWS CORE MELT SEQUENCE 21 FOR T_{2A} TRANSIENTS
ε
RPS FAILS
ε
(From App. A)
NORMAL HEAT REMOVAL FAILS
1.0
(By Definition)
VESSEL INTEGRITY FAILS
0.5
(From Text)
HPI FAILS
High
(Due to LOSP)
T_{2A} TRANSIENT OCCURS
0.32/Year
(From Table 4.1)

FIGURE 5.5. QUANTIFICATION ILLUSTRATION FOR ATWS CORE MELT SEQUENCE 21 FOR ALL TRANSIENT INITIATORS

The CR-3 event tree accident sequences whose calculated frequencies are greater than the cutoff value (1E-7/yr) were matched with possible containment failure modes and assigned to release categories by comparing the sequences with similar sequences appearing in the Reactor Safety Study Methodology Applications Program (RSSMAP) analysis of the Oconee-3 plant (5-18). Table 5.11 shows[1], for LOCA initiated accidents, a comparison of the CR-3 sequences (column 1), and the Oconee sequences (column 2), and the assigned release category(s) and probability (ies) corresponding to various containment failure modes. In general, each event tree sequence could result in several possible accident sequences depending on the containment failure mode. The evaluation of each such accident sequence simply involved multiplying the initiating event probability, the event tree sequence probability and the containment failure mode probability from Table 5.10. Table 5.12 shows a similar correspondence among the CR-3 and Oconee transient sequences, and the release categories. The transient sequences were quantified in the same way as the LOCA sequences.

5.3.6 Accident Sequence Analysis Results

Tables 5.13 through 5.20 list the probability of each accident sequence, not including containment failure probabilities, for both transient-induced and spontaneous LOCAs. The LOCA sequence numbers, corresponding to each sequence on the LOCA event tree are given in the first column; the outcomes in terms of core melt or safe[2] sequences are presented in column two. The third column presents the conditional probability of the event sequence, given the initiating event. In the case of transient-induced LOCAs, the initiating event consists of both the accident initiator (T_X) and the generic transient sequence leading to the LOCA, which is a stuck open safety valve. Column four presents the probabilities of each LOCA sequence including, for the transient-induced LOCAs, the frequency of the accident initiator and the probability of the generic sequence; and for pipe breaks, the probability of a pipe break of the stated size. Containment failure probabilities are not included in these tables. Sequence probabilities of less than 1.0 E-7 were recorded as ε.

---

[1] Table 5.11 and all subsequent tables in Section 5.3 appear at the end of the section.

[2] Safe, when used in reference to a sequence outcome, is defined as a non-melt result. No distinction is made between sequences resulting in no fuel cladding damage and those resulting in fuel cladding damage short of core melt.

Table 5.21 lists the conditional sequence probability for each of the transient sequences of interest that does not result in a LOCA, but could lead to core melt. Three such sequences are of interest (listed as T_8, T_9, T_{10}) for each of the transient initiators. Sequence T_8 represents failure of normal and emergency secondary heat removal, and failure to establish feed and bleed. Sequence T_9 represents all the failures in sequence T_8, plus failure of containment radioactivity removal. Sequence T_{10} represents all the failures of sequence T_9 plus failure of containment cooling.

The conditional sequence probabilities listed in the fourth column are the probability of the sequence given (1) the initiating event, (2) that pressure relief is successful (event $\overline{P}_2$), (3) that a nonmitigable LOCA does not occur (event $\overline{Q}$), and (4) that PCS is not available as the accident progresses. The sequence probabilities listed in the last column include the probabilities of those events which are mentioned as "given" above. As in the previous tables, containment failure mode probabilities are not included.

The sequences were combined with containment failure modes and assigned to release categories. The release categories used were described in Section 4.6. The results are presented in Tables 5.22 and 5.23 which list the accident sequences contributing to each release category, by accident initiator, for transient-initiated and LOCA-initiated events, respectively.

The sequences whose probabilities appear to be dominant in each release category for the aggregate of all transient and LOCA initiators are identified in Table 5.24 and listed by decreasing order-of-magnitude of the estimated individual sequence probabilities. The dominant risk for the CR-3 plant, when consideration is given to both accident sequence point estimates and release categories, appears to be due to the sequences shown in this table in release categories one through three.

All of the highest frequency sequences shown in these categories are initiated by small-small (B_4) LOCAs or loss-of-offsite-power (T_{2A}) transients. In fact, about one-half of the sequences in this table have these initiators and account for over 85% of the total core melt probability. The preponderance of these initiators is more dramatically presented in Tables 5.22 and 5.23, where it is clearly shown that the B_4 LOCA and the T_{2A} transient initiators dominate the low-numbered, high-consequence release categories. These results can be generally attributed to several causes: The B_4 LOCA sequences are dominated by high probability operator errors. Other contributors arise from the fact that the frequency of this initiator was assessed an order-of-magnitude higher than the other LOCA sizes, and a B_4 LOCA requires successful operation of both the high pressure injection system and the low pressure injection system (for recirculation) to prevent core melt. The T_{2A} (LOSP) transient initiator's significance is largely due to its relatively high frequency of 0.32/reactor year, the pervasive nature of AC power requirements in the plant, and the relatively high unavailabilities of emergency AC power from CR-1 and CR-2, the CR-3 diesel-generators, and the turbine-driven emergency feedwater train.

The B_4S_2 and B_4S_{23} sequences appear in three release categories each with different containment failure modes in each of the categories. Both of these B_4 LOCA initiated sequences are dominated by accident sequence cut sets which contain various types of operator errors, as described in Section 2.2.

The $T_{2A}T_8$, $T_{2A}T_9$, and $T_{2A}T_{10}$ sequences are nearly identical differing only in the success or failure of the containment functions of pressure reduction and/or post accident radioactivity removal. The $T_{2A}T_{11}S_{27}$ sequence is very similar, differing from the others in that it also includes a stuck-open safety valve. These transient-initiated dominant sequences are dominated by two accident sequence cut sets:

- Loss of offsite power, failure of Battery B, and failure to obtain emergency back-up power on AC power Train A.

- Loss of offsite power, failure to obtain emergency power on either AC power train, and failure of the EFS turbine pump.

Each of these two cut sets results in total loss of AC power and loss of the EFS turbine pump. A more detailed description of each of the dominant sequences in Table 5.24 is contained in Section 2.2, and a discussion of potential approaches for reducing the point estimate probabilities for some of the dominant sequences is given in Section 2.3.

BEST DOCUMENT AVAILABLE

Table 5.11 Correspondence Between CR-3 and Oconee LOCA Sequences by Containment Failure Modes and Release Category[1]

CR-3 LOCA Sequence	Oconee LOCA Sequence	Reactor Safety Study Radioactivity Release Categories for PWR						
		1	2	3	4	5	6	7
B_1S_2	AH	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_1S_6	AFH	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_1S_9	AD	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_1S_{23}	ACD	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_2S_2	S_1H	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_2S_6	S_1FH	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_2S_9	S_1D	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_2S_{23}	S_1CD	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_3S_2	S_2H	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_3S_6	S_2FH	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_3S_9	S_2D	$\alpha = .01$		$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$
B_3S_{23}	S_2CD	$\alpha = .01$	$\gamma = 0.2$		$\beta = .007$		$\epsilon = 0.8$	
B_4S_2	S_3H	$\alpha = .0001$		$\gamma = 0.5$		$\beta = .007$		$\epsilon = 0.5$
B_4S_6	S_3FH	$\alpha = .0001$	$\gamma = 0.5$		$\beta = .007$		$\epsilon = 0.5$	
B_4S_9	S_3D	$\alpha = .0001$		$\gamma = 0.5$		$\beta = .007$		$\epsilon = 0.5$
B_4S_{14}	S_3YH	$\alpha = .0001$		$\gamma = 0.5$		$\beta = .007$	$\delta = 0.5$	
B_4S_{20}	S_3CH	$\alpha = .0001$	$\gamma = 0.5$		$\beta = .007$		$\epsilon = 0.5$	
B_4S_{23}	S_3CD	$\alpha = .0001$	$\gamma = 0.5$		$\beta = .007$		$\epsilon = 0.5$	
B_4S_{27}	S_3CYD	$\alpha = .0001$	$\delta = 0.5$		$\beta = .007$		$\epsilon = 0.5$	

12/1/81

---

[1] This table includes only CR-3 LOCA sequences with calculated frequencies $\geq$ 1E-7/Reactor-Year, the cutoff value used in the sequence quantification.

Table 5.12 Correspondence Between CR-3 and Oconee Transient Sequences by Containment Failure Modes and Release Category[1]

CR-3 Transient Sequence	Oconee Transient Sequence	Reactor Safety Study Radioactivity Release Categories for PWR						
		1	2	3	4	5	6	7
$T_{2A}T_8$	$T_1(B_3)$MLU	α = .0001		γ = 0.5		β = .007		ε = 0.5
$T_{2A}T_9$	$T_1(B_3)$MLUO'	α = .0001	γ = 0.5		β = .007		ε = 0.5	
$T_{2A}T_{10}$	$T_1(B_3)$MLUOO'	α = .0001	δ = 0.5		β = .007		ε = 0.5	
$T_{2A}T_{11}S_2$	T_1MLQH	α = .0001		γ = 0.5		β = .007		ε = 0.5
$T_{2A}T_{11}S_9$	$T_1(B_3)$MLQD	α = .0001		γ = 0.5		β = .007		ε = 0.5
$T_{2A}T_{11}S_{23}$	$T_1(B_3)$MLQCD	α = .0001	γ = 0.5		β = .007		ε = 0.5	
$T_{2A}T_{11}S_{27}$	$T_1(B_3)$MLQCYD	α = .0001	δ = 0.5		β = .007		ε = 0.5	
$(T_2-T_{2A})T_8$	T_2MLU	α = .0001		γ = 0.5		β = .007		ε = 0.5
$(T_2-T_{2A})T_{11}S_2$	T_2MLQH	α = .0001		γ = 0.5		β = .007		ε = 0.5
$(T_2-T_{2A})T_{11}S_9$	T_2MLQD	α = .0001		γ = 0.5		β = .007		ε = 0.5
$(T_2-T_{2A})T_{11}S_{23}$	T_2MLQCD	α = .0001	γ = 0.5		β = .007		ε = 0.5	
$(T_1-T_{1A})T_8$	T_3MLU	α = .0001		γ = 0.5		β = .007		ε = 0.5
$(T_1-T_{1A})T_{11}S_2$	T_3MLQH	α = .0001		γ = 0.5		β = .007		ε = 0.5
$(T_1-T_{1A})T_{11}S_{23}$	T_3MLQCD	α = .0001	γ = 0.5		β = .007		ε = 0.5	

12/1/81

---

[1] This table includes only CR-3 transient sequences with calculated frequencies ≥ 1E-7/Reactor-Year, the cutoff value used in the sequence quantification.

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table 5.13 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_1-T_{1A} Transient Initiators

INITIATOR: $T_X = T_1$-T_{1A} (ANY TRANSIENT, OTHER THAN LOSS OF NSCCCWS, WHICH LEAVES PCS AVAILABLE)			
		LOCA INDUCED FROM T SEQ. #11 (EFS FAILURE)	
LOCA SEQUENCE NUMBER	OUTCOME[1, 2]	CONDITIONAL PROBABILITY $P(S_XL\|T_XMQ)$	SEQUENCE PROBABILITY $P(S_XL\|T_XMQ) \cdot P(MQ) \cdot F(T_X)$
2	CM	4.4 E-5	7.5 E-7
3	S		ε
4	CM	ε	ε
5	S		
6	CM	1.1 E-6	ε
7	CM ?	ε	ε
8	CM	ε	ε
9	CM	2.3 E-6	ε
10	CM	ε	ε
11	CM	ε	ε
12	CM	ε	ε
13	S		
14	CM	1.1 E-7	ε
15	CM ?	ε	ε
16	CM	ε	ε
17	CM	ε	ε
18	CM	ε	ε
19	S		
20	CM	2.2 E-7	ε
21	CM ?	ε	ε
22	CM	ε	ε
23	CM	1.7 E-5	2.9 E-7
24	CM	ε	ε
25	CM ?	ε	ε
26	CM	ε	ε
27	CM	ε	ε

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

Table 5.14 Probabilities for Transient Induced S_4 LOCA Accident Sequences for Type T_{1A} Transient Initiators

INITIATOR: $T_X = T_{1A}$ (LOSS OF NSCCCWS, PCS AVAILABLE)			
		LOCA INDUCED FROM T SEQ. #11 (EFS FAILURE)	
LOCA SEQUENCE NUMBER	OUTCOME[1,2,3]	CONDITIONAL PROBABILITY $P(S_XL\|T_XMQ)$	SEQUENCE PROBABILITY $P(S_XL\|T_XMQ)\cdot P(MQ)\cdot F(T_X)$
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13	S		
14	CM	5.4 E-5	ε
15	CM ?	3.5 E-7	ε
16	CM	1.1 E-6	ε
17	CM	1.1 E-5	ε
18	CM	ε	ε
19			
20			
21			
22			
23			
24			
25	CM ?	3.4 E-6	ε
26	CM	1.3 E-6	ε
27	CM	1.7 E-5	ε

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

[3] Sequences for which no outcome is shown are not physically possible.

BEST DOCUMENT AVAILABLE

BEST DOCUMENT AVAILABLE

Table 5.15 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_2-T_{2A} Transient Initiators

INITIATOR: $T_X = T_2$-T_{2A} (ANY TRANSIENT OTHER THAN LOSS OF OFFSITE POWER, WHICH LEAVES PCS NOT AVAILABLE)			
		LOCA INDUCED FROM T SEQ. #11 (EFS FAILURE)	
LOCA SEQUENCE NUMBER	OUTCOME[1,2]	CONDITIONAL PROBABILITY $P(S_XL \mid T_XMQ)$	SEQUENCE PROBABILITY $P(S_XL \mid T_XMQ) \cdot P(LQ) \cdot F(T_X)$
2	CM	4.4 E-5	2.5 E-6
3	S		
4	CM	ϵ	ϵ
5	S		
6	CM	1.1 E-6	ϵ
7	CM ?	ϵ	ϵ
8	CM	ϵ	ϵ
9	CM	2.3 E-6	1.3 E-7
10	CM	ϵ	ϵ
11	CM	ϵ	ϵ
12	CM	ϵ	ϵ
13	S		
14	CM	1.1 E-7	ϵ
15	CM ?	ϵ	ϵ
16	CM	ϵ	ϵ
17	CM	ϵ	ϵ
18	CM	ϵ	ϵ
19	S		
20	CM	2.2 E-7	ϵ
21	CM ?	ϵ	ϵ
22	CM	ϵ	ϵ
23	CM	1.7 E-5	9.7 E-7
24	CM	ϵ	ϵ
25	CM ?	ϵ	ϵ
26	CM	ϵ	ϵ
27	CM	ϵ	ϵ

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

8/11/81

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.16 Probabilities for Transient Induced B_4 LOCA Accident Sequences for Type T_{2A} Transient Initiators

INITIATOR: $T_X = T_{2A}$ (LOSS OF OFFSITE POWER, PCS NOT AVAILABLE)			
		LOCA INDUCED FROM T SEQ. #11 (EFS FAILURE)	
LOCA SEQUENCE NUMBER	OUTCOME[1,2]	CONDITIONAL PROBABILITY $P(S_XL \mid T_XMQ)$	SEQUENCE PROBABILITY $P(S_XL \mid T_XMQ) \cdot P(LQ) \cdot F(T_X)$
2	CM	1.4 E-4	8.9 E-7
3	S		
4	CM	ε	ε
5	S		
6	CM	2.6 E-6	ε
7	CM ?	ε	ε
8	CM	ε	ε
9	CM	3.4 E-5	2.2 E-7
10	CM	ε	ε
11	CM	ε	ε
12	CM	ε	ε
13	S		
14	CM	ε	ε
15	CM ?	ε	ε
16	CM	ε	ε
17	CM	2.3 E-7	ε
18	CM	ε	ε
19	S		
20	CM	1.1 E-7	ε
21	CM ?	ε	ε
22	CM	ε	ε
23	CM	6.8 E-5	4.3 E-7
24	CM	ε	ε
25	CM ?	ε	ε
26	CM	ε	ε
27	CM	1.6 E-4	1.0 E-6

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.17 Probabilities for B_1 Accident Sequences

SEQUENCE NUMBER	OUTCOME[1,2]	CONDITIONAL PROBABILITY $P(S_X\|B_1)$	SEQUENCE PROBABILITY $P(S_X\|B_1)\cdot P(B_1)$
2	CM	1.0 E-3	1.0 E-7
3	S		
4	CM	ε	ε
5	S		
6	CM	3.0 E-3	3.0 E-7
7	CM ?	ε	ε
8	CM	ε	ε
9	CM	5.0 E-2	5.0 E-6
10	CM	1.2 E-5	ε
11	CM	2.0 E-4	ε
12	CM	ε	ε
13	S		
14	CM	2.1 E-6	ε
15	CM ?	2.1 E-6	ε
16	CM	6.3 E-6	ε
17	CM	1.4 E-4	ε
18	CM	ε	ε
19	S		
20	CM	ε	ε
21	CM ?	ε	ε
22	CM	ε	ε
23	CM	5.0 E-2	5.0 E-6
24	CM	1.2 E-5	ε
25	CM ?	ε	ε
26	CM	ε	ε
27	CM	1.4 E-5	ε

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.18 Probabilities for B_2 Accident Sequences

SEQUENCE NUMBER	OUTCOME[1, 2]	CONDITIONAL PROBABILITY $P(S_X\|B_2)$	SEQUENCE PROBABILITY $P(S_X\|B_2)\cdot P(B_2)$
2	CM	1.0 E-3	1.0 E-7
3	S		
4	CM	ϵ	ϵ
5	S		
6	CM	3.0 E-3	3.0 E-7
7	CM ?	ϵ	ϵ
8	CM	ϵ	ϵ
9	CM	5.0 E-2	5.0 E-6
10	CM	1.2 E-5	ϵ
11	CM	2.0 E-4	ϵ
12	CM	ϵ	ϵ
13	S		
14	CM	2.1 E-6	ϵ
15	CM ?	2.1 E-6	ϵ
16	CM	6.3 E-6	ϵ
17	CM	1.4 E-4	ϵ
18	CM	ϵ	ϵ
19	S		
20	CM	ϵ	ϵ
21	CM ?	ϵ	ϵ
22	CM	ϵ	ϵ
23	CM	5.0 E-2	5.0 E-6
24	CM	1.2 E-5	ϵ
25	CM ?	ϵ	ϵ
26	CM	ϵ	ϵ
27	CM	1.4 E-5	ϵ

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.19 Probabilities for B_3 Accident Sequences

SEQUENCE NUMBER	OUTCOME[1, 2]	CONDITIONAL PROBABILITY $P(S_X \mid B_3)$	SEQUENCE PROBABILITY $P(S_X \mid B_3) \cdot P(B_3)$
2	CM	1.0 E-3	1.0 E-7
3	S		
4	CM	ϵ	ϵ
5	S		
6	CM	3.0 E-3	3.0 E-7
7	CM ?	ϵ	ϵ
8	CM	ϵ	ϵ
9	CM	5.7 E-2	5.7 E-6
10	CM	1.4 E-5	ϵ
11	CM	2.3 E-4	ϵ
12	CM	ϵ	ϵ
13	S		
14	CM	2.1 E-6	ϵ
15	CM ?	2.1 E-6	ϵ
16	CM	6.3 E-6	ϵ
17	CM	1.6 E-4	ϵ
18	CM	ϵ	ϵ
19	S		
20	CM	3.0 E-5	ϵ
21	CM ?	2.4 E-6	ϵ
22	CM	ϵ	ϵ
23	CM	5.1 E-2	5.1 E-6
24	CM	1.2 E-5	ϵ
25	CM ?	2.7 E-5	ϵ
26	CM	ϵ	ϵ
27	CM	1.4 E-4	ϵ

8/11/81

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.20 Probabilities for B_4 Accident Sequences

SEQUENCE NUMBER	OUTCOME[1, 2]	CONDITIONAL PROBABILITY $P(S_X\|B_4)$	SEQUENCE PROBABILITY $P(S_X\|B_4) \cdot P(B_4)$
2	CM	1.3 E-1	1.7 E-4
3	S		
4	CM	3.2 E-5	ϵ
5	S		
6	CM	3.1 E-3	4.0 E-6
7	CM ?	ϵ	ϵ
8	CM	ϵ	ϵ
9	CM	6.9 E-3	9.0 E-6
10	CM	1.6 E-6	ϵ
11	CM	2.6 E-5	ϵ
12	CM	ϵ	ϵ
13	S		
14	CM	3.1 E-4	4.0 E-7
15	CM ?	2.1 E-6	ϵ
16	CM	6.3 E-6	ϵ
17	CM	1.9 E-5	ϵ
18	CM	ϵ	ϵ
19	S		
20	CM	6.4 E-4	8.3 E-7
21	CM ?	2.4 E-6	ϵ
22	CM	ϵ	ϵ
23	CM	5.0 E-2	6.5 E-5
24	CM	1.2 E-5	ϵ
25	CM ?	2.7 E-5	ϵ
26	CM	ϵ	ϵ
27	CM	1.4 E-4	1.8 E-7

8/11/81

---

[1] No results are provided for sequences which result in a safe (S) outcome (i.e., the non-core-melt sequences).

[2] Sequences for which the outcome is shown as "CM?" may not result in a core melt; however, they are conservatively assumed to result in core melt for the purposes of this analysis.

BEST DOCUMENT AVAILABLE

Table 5.21 Non-LOCA Transient Sequence Probabilities

TRANSIENT INITIATOR (T_x)	TRANSIENT SEQUENCE (T_s)	OUTCOME	CONDITIONAL PROBABILITY $P(T_s \mid M\bar{P}_2\bar{Q}T_x)$	SEQUENCE PROBABILITY $P(T_s \mid M\bar{P}_2\bar{Q}T_x)\cdot P(M\bar{P}_2\bar{Q})\cdot P(T_x)$
T_{1A}	T_8	CM	1.4 E-5	ϵ
	T_9	CM	Not Possible	Not Possible
	T_{10}	CM	2.0 E-7	ϵ
T_1-T_{1A}	T_8	CM	4.8 E-6	4.1 E-6
	T_9	CM	ϵ	ϵ
	T_{10}	CM	ϵ	ϵ
T_{2A}	T_8	CM	4.3 E-5	1.4 E-5
	T_9	CM	7.7 E-6	2.5 E-6
	T_{10}	CM	1.7 E-4	5.4 E-5
T_2-T_{2A}	T_8	CM	4.8 E-6	8.6 E-6
	T_9	CM	ϵ	ϵ
	T_{10}	CM	ϵ	ϵ

8/11/81

BEST DOCUMENT AVAILABLE

Table 5.22 Dominant Accident Sequences vs Release Categories for Transient-Inititated Events (Including Transient Induced LOCAs)

INITIATING EVENT	RSS RADIOACTIVITY RELEASE CATEGORIES FOR PWR						
	1	2	3	4	5	6	7
T_{1A}	← NONE →						
T_1-T_{1A}		$T_{11}S_{23}-\gamma$ 1.5 E-7	$T_8-\gamma$ 2.1 E-6 $T_{11}S_2-\gamma$ 3.8 E-7			$T_{11}-S_{23}-\epsilon$ 1.5 E-7	$T_8-\epsilon$ 2.1 E-6 $T_{11}S_2-\epsilon$ 3.8 E-7
I.E. TOTALS		2E-7	2.5 E-6			2E-7	2.5 E-6
T_{2A}		$T_{10}-\delta$ 2.7 E-5 $T_9-\gamma$ 1.3 E-6 $T_{11}S_{27}-\delta$ 5.0 E-7 $T_{11}S_{23}-\gamma$ 2.2 E-7	$T_8-\gamma$ 7.0 E-6 $T_{11}-S_2-\gamma$ 4.5 E-7 $T_{11}-S_9-\gamma$ 1.1 E-7	$T_{10}-\beta$ 3.8 E-7	$T_8-\beta$ ≤ 1E-7	$T_{10}-\epsilon$ 2.7 E-5 $T_9-\epsilon$ 1.3 E-6 $T_{11}S_{27}-\epsilon$ 5.0 E-7 $T_{11}S_{23}-\epsilon$ 2.2 E-7	$T_8-\epsilon$ 7.0 E-6 $T_{11}S_2-\epsilon$ 4.5 E-7 $T_{11}S_9-\epsilon$ 1.1 E-7
I.E. TOTALS		2.9 E-5	7.6 E-6	4E-7	1E-7	2.9 E-5	7.6 E-6
T_2-T_{2A}		$T_{11}S_{23}-\gamma$ 4.9 E-7	$T_8-\gamma$ 4.3 E-6 $T_{11}S_2-\gamma$ 1.3 E-6 $T_{11}S_9-\gamma$ ≤ 1E-7			$T_{11}S_{23}-\epsilon$ 4.9 E-7	$T_8-\epsilon$ 4.3 E-6 $T_{11}S_2-\epsilon$ 1.3 E-6 $T_{11}S_9-\epsilon$ ≤ 1E-7
I.E. TOTALS		5E-7	5.7 E-6			5E-7	5.7 E-6
TRANSIENT TOTALS	See Note 1	3.0 E-5	1.6 E-5	4E-7	1E-7	3.0 E-5	1.6 E-5

11/23/81

---

[1] On the order of 1E-7, the cutoff value used in the sequence quantification.

[redacted]

BEST DOCUMENT AVAILABLE

Table 5.23 Dominant Accident Sequences vs Release Categories for LOCA Initiated Events

INITIATING EVENT	RSS RADIOACTIVITY RELEASE CATEGORIES FOR PWR						
	1	2	3	4	5	6	7
B_1		S_{23}-γ 1.0 E-6	S_9-γ 1.0 E-6 S_6-γ ≤ 1E-7			S_{23}-ε 4.0 E-6 S_6-ε 2.4 E-7	S_9-ε 4.0 E-6 S_2-ε 1E-7
I.E. TOTALS		1.0 E-6	1.1 E-6			4.2 E-6	4.1 E-6
B_2		S_{23}-γ 1.0 E-6	S_9-γ 1.0 E-6 S_6-γ ≤ 1E-7			S_{23}-ε 4.0 E-6 S_6-ε 2.4 E-7	S_9-ε 4.0 E-6 S_2-ε ≤ 1E-7
I.E. TOTALS		1.0 E-6	1.1 E-6			4.2 E-6	4.1 E-6
B_3		S_{23}-γ 1.0 E-6	S_9-γ 1.1 E-6 S_6-γ ≤ 1E-7			S_{23}-ε 4.1 E-6 S_6-ε 2.4 E-7	S_9-ε 4.6 E-6 S_2-ε ≤ 1E-7
I.E. TOTALS		1.0 E-6	1.2 E-6			4.3 E-6	4.7 E-6
B_4		S_{23}-γ 3.3 E-5 S_6-γ 2.0 E-6 S_{20}-γ 4.2 E-7 S_{27}-δ ≤ 1E-7	S_2-γ 8.5 E-5 S_9-γ 4.5 E-6 S_{14}-γ 2.0 E-7	S_{23}-β 4.6 E-7	S_2-β 1.2 E-6	S_{23}-ε 3.3 E-5 S_6-ε 2.0 E-6 S_{20}-ε 4.2 E-7 S_{14}-δ 2.0 E-7 S_{27}-ε ≤ 1E-7	S_2-ε 8.5 E-5 S_9-ε 4.5 E-6
I.E. TOTALS		3.6 E-5	9.0 E-5	5E-7	1.2 E-6	3.6 E-5	9.0 E-5
LOCA TOTALS	See Note 1	3.9 E-5	1.2 E-4	5E-7	1.2 E-6	4.9 E-5	1.0 E-4

11/23/81

[1] On the order of 1E-7, the cutoff value used in the sequence quantification.

BEST DOCUMENT AVAILABLE

Table 5.24 Dominant Accident Sequences vs Release Categories Tabulated in Decreasing Order-of-Magnitude of Sequence Probabilities

RELEASE CATEGORY	RSS RADIOACTIVITY RELEASE CATEGORIES FOR PWR						
	1	2	3	4	5	6	7
$\geq 10^{-4}$							
$\geq 10^{-5}$		$B_4S_{23}-\gamma$ 3.3 E-5 $T_{2A}T_{10}-\delta$ 2.7 E-5	$B_4S_2-\gamma$ 8.5 E-5			$B_4S_{23}-\epsilon$ 3.3 E-5 $T_{2A}T_{10}-\epsilon$ 2.7 E-5	$B_4S_2-\epsilon$ 8.5 E-5
$\geq 10^{-6}$		$B_4S_6-\gamma$ 2.0 E-6 $T_{2A}T_9-\gamma$ 1.3 E-6 $B_3S_{23}-\gamma$ 1.0 E-6 $B_2S_{23}-\gamma$ 1.0 E-6 $B_1S_{23}-\gamma$ 1.0 E-6	$T_{2A}T_8-\gamma$ 7.0 E-6 $B_4S_9-\gamma$ 4.5 E-6 $(T_2-T_{2A})T_8-\gamma$ 4.3 E-6 $(T_1-T_{1A})T_8-\gamma$ 2.1 E-6 $(T_2-T_{2A})T_{11}S_2-\gamma$ 1.3 E-6 $B_3S_9-\gamma$ 1.1 E-6 $B_2S_9-\gamma$ 1.0 E-6 $B_1S_9-\gamma$ 1.0 E-6		$B_4S_2-\beta$ 1.2 E-6	$B_3S_{23}-\epsilon$ 4.1 E-6 $B_2S_{23}-\epsilon$ 4.0 E-6 $B_1S_{23}-\epsilon$ 4.0 E-6 $B_4S_6-\epsilon$ 2.0 E-6 $T_{2A}T_9-\epsilon$ 1.3 E-6	$T_{2A}T_8-\epsilon$ 7.0 E-6 $B_3S_9-\epsilon$ 4.6 E-6 $B_4S_9-\epsilon$ 4.5 E-6 $(T_2-T_{2A})T_8-\epsilon$ 4.3 E-6 $B_2S_9-\epsilon$ 4.0 E-6 $B_1S_9-\epsilon$ 4.0 E-6 $(T_1-T_{1A})T_8-\epsilon$ 2.1 E-6 $(T_2-T_{2A})T_{11}S_2-\epsilon$ 1.3 E-6
$\geq 10^{-7}$				$B_4S_{23}-\beta$ 4.6 E-7 $T_{2A}T_{10}-\beta$ 3.8 E-7	$T_{2A}T_8-\beta$ $\leq$ 1E-7		
TOTALS (APPROXIMATE)	See Note 1	6.6 E-5	1.1 E-4	8E-7	1.3 E-6	7.5 E-5	1.2 E-4
Total Probability of Core Melt $\approx$ 3.7 E-4							

11/23/81

---

[1] On the order of 1E-7, the cutoff value used in the sequence quantification.

5.4 Analysis of Selected Operator Faults

Six of the most easily identifiable important operator faults are singled out for special attention. Five of these contribute to LOCA sequences while the sixth contributes to transient sequences with loss of all secondary cooling. Of the five LOCA-related faults, three are dominant contributors to dominant sequences; the other two are closely related faults although not as significant quantitatively. The transient fault illustrates the role of the operator as a backup to automatic systems. Because of the importance of these faults, the object of this analysis is to improve the accuracy of their estimated probabilities, or at least to increase the confidence that might be placed in an assertion that the estimated probabilities are of the correct order of magnitude. Whether or not the objective is met, the analysis should illustrate both the importance of operator faults and the pitfalls associated with estimating their probabilities.

The six faults are identified by their Boolean variable name and defined below. The estimated probabilities are given in parentheses following each definition:

H*02	Operator makes error in switching to recirculation and loses core cooling capability, given a B_4 or transient-induced LOCA (0.08)
L06	Premature cutoff of low pressure coolant injection by operator, given a LOCA (0.05)
L017	Premature initiation of recirculation, given a LOCA (0.05)
L04	Delayed initiation of recirculation, given a LOCA (0.003)
H01	Premature cutoff of high pressure coolant injection by operator, given B_4, B_3 or transient-induced LOCA (0.004)
H03	Failure to establish a "feed and bleed" operation, given a transient with loss of all secondary cooling (0.014)

All of these faults pertain to specific actions required of the operator as set forth in various emergency procedures. All of the faults imply a failure to recover.

Each fault is analyzed by breaking down each complex action (as described in the appropriate procedure) into a sequence of independent simpler actions such that all the simple actions must be performed correctly and in order. Failure to perform any one of the simple actions results in failure of the complex action. In fault tree terminology, the complex fault is represented as a single OR gate with all the simple faults as inputs. For analytical purposes, simple (proper) actions are denoted by lower case letters and the simple faults by the corresponding upper case letters. For example, let a successful complex action $\overline{X}$, with failure X, be comprised of three simple actions, a, b, and c. The Boolean equations are then:

$$\overline{X} = a \cdot b \cdot c \quad ; \quad X = A + B + C$$

and the probability of the fault X is

$$\begin{aligned} P(X) &= 1-P(a \cdot b \cdot c) \\ &= 1-[1-P(A)][1-P(B)]\ [1-P(C)] \end{aligned}$$

Applying the small probability approximation, for all practical purposes the last expression becomes:

$$P(X) \approx P(A) + P(B) + P(C)$$

The generalization to events with more than three simple actions is obvious. The theory is that the probabilities of the simple faults can be estimated more reliably than can the complex fault considered as a single event.

The logical structure of a complex fault may be illustrated by a simple tree-like diagram, with branches to the left for successes and to the right for failures. Such trees are shown in Figures 5-6 through 5-11, which summarize the analyses of the six faults under consideration[1]. Branches are labeled with symbols as indicated above and probabilities for each branch are shown in parentheses.

---

[1] These figures appear at the end of Section 5.4

The simple required actions (a, b, c...) which comprise the complete fault are defined immediately below the tree diagram. The simple faults (A, B, C...) are not defined explicitly; they are simply the complements of the required actions.

These figures are intended to be more or less self-explanatory, more if the appropriate procedures and other references are at hand. These analyses are examples of a technique called THERP (Technique for Human Error Rate Prediction) as described in Reference 5-10 (NUREG/CR-1278). This document provides extensive tables and guidelines for estimating the probabilities of simple faults. When a particular simple fault is represented explicitly in NUREG/CR-1278, the given central estimate is used unless otherwise indicated in the figures. The specific table and line number is generally shown under "Sources or Bases for Probabilities"; if the explanation begins with "Estimate", it means the fault is not explicitly represented in NUREG/CR-1278, in which case the fault is compared to a similar or related fault appearing in the tables, which is then indicated, or the probability is simply estimated on the basis of "engineering judgment" tempered with some human factors experience.

A small-small LOCA followed by successful coolant injection but subsequent failure of core cooling in recirculation (sequence B_4S_2) is one of the most important sequences because it is dominant in several release categories, depending on the containment failure mode. The operator faults H*02 and L06 together contribute about 97% to the conditional (given the initiating event) probability of this sequence. Both faults are singles to the LOCA sequence S_2.

H*02 (contributing about 59% to $P(S_2)$) involves a complex action with many opportunities for making a mistake. The analysis in Figure 5.6 suggests that the arrangement of control panels should be examined with respect to this and similar types of fault. The fault L06 (contributing about 38% to $P(S_2)$) involves a rather simple action in itself (although it is embedded in a much more complex action), but the required action is contrary to what is required in many similar situations, even those occurring in the larger context in which the fault L06 is embedded. It raises questions about such procedures, or about systems designs which call for such procedures.

The operator fault L017 is closely related to H*02 and L06. It contributes essentially 100% to LOCA sequence S_{23}. This sequence is not the most dominant in any category but it is a significant contributor to several. L017 also contributes significantly to the LOCA sequence S_{27}, which entails failure of all cooling systems in injection (and therefore in recirculation). L017 itself fails emergency coolant injection (both low and high pressure) and reactor building spray injection. It must combine with a fault (most likely a valve or valve-related failure) in the Reactor Building Emergency Cooling System to cause the sequence S_{27}. With these combinations considered, L017 is involved in contributing about 92% to the probability of S_{27}, or of B_4S_{27}.

L04 is not a major contributor to dominant sequences, but it is a counterpart to L017. As are all the LOCA-related faults, these are embedded in an extensive set of procedures for coping with a LOCA. It may be of interest to note that L017 is treated as an injection fault and L04 as a recirculation fault. This somewhat artificial distinction stems from the tacit assumption of a sharp dividing line between injection and recirculation. For either fault, the result is a loss of suction to the low pressure pumps and subsequent cavitation and burnout.

The fault H01 is a major contributor (about 50%) to the LOCA sequence S_9. The sequence $B_4S_9-\epsilon$ is one of the dominant sequences appearing in release category 7. There is no doubt that such a fault could happen because it did happen at TMI (5-19). On the other hand, it is much less likely to happen again (given a demand for HPI) because of TMI. Reactor operators everywhere are presumably sensitized to the possible consequences of turning off HPI. Moreover, an NRC regulation now explicitly prohibits turning off HPI for twenty minutes after it is initiated automatically.

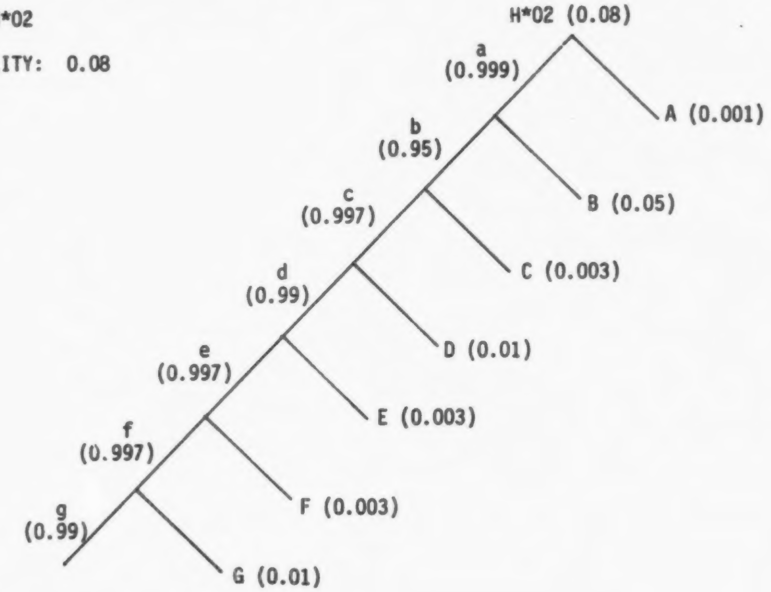
Finally, the fault H03 is a different type of fault. It could arise in the event of a transient with subsequent loss of both normal and emergency secondary cooling, i.e., loss of all feedwater flow to the steam generators. The only way to cool the reactor would be to remove energy by blowing off steam through a relief valve and replenishing the water inventory by means of the high pressure injection pumps. Such an operation is referred to as a "feed and bleed" operation. It is a manual operation performed by the operator from the control room. The fault H03 is failure to (a) diagnose the need for "feed and bleed" or (b) properly initiate the operation. The feed and bleed operation under the indicated circumstances is possible with B&W reactors because the B&W HPI pumps have such a high shutoff head that they can pump large amounts of coolant into the reactor even at normal operating pressures, whereas other PWR HPI pumps have shutoff heads substantially below normal operating pressures; in a sense this helps to compensate for the rapid response of the once-through steam generator to feedwater transients, but it must be initiated within a time window of about 20 minutes. (Other PWRs permit a much longer time window, which increases the chances of recovering emergency feedwater flow.)

H03, in combination with other faults, is a significant contributor to the sequence $T_{2A}T_8 - \epsilon$, which is dominant in the seventh release category. The combination of faults most likely to yield this sequence include loss of offsite power (the initiating event), failure of emergency diesel "A", failure of emergency backup power from Crystal River Units 1 and 2, failure of the turbine-driven emergency feedwater train and H03. It may be of interest to note that the same combinations of faults, except with H03 replaced by the human fault of leaving one-of-two manual valves closed in the high pressure train B, makes a comparable (actually larger) contribution to the sequence probability.

FAULT: Operator makes error in switching to recirculation and loses core cooling capability, given a B4 or transient-induced LOCA

BOOLEAN SYMBOL: H*02

ESTIMATED PROBABILITY: 0.08



REQUIRED ACTIONS:

a: Operator opens at least one DHP suction to RB sump
b: Operator opens at least one DHP discharge to MUP suction
c: Operator performs step to close DHP suction from BWST
d: Operator closes second DHP suction, given that he has closed first
e: Operator starts at least one DHP
f: Operator performs step to close MUP suction from BWST
g: Operator closes second MUP suction, given that he has closed first

ASSUMPTIONS:

1. Analysis based on one operator
2. The probabilities of inadvertently selecting an incorrect control is assumed negligible.

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: Estimate. NUREG/CR-1278, Table 20-20, line 4; because of BWST alarm, treat as short procedure, and use low value because the first item in a list is the least likely to be omitted.
b,B: Estimate. Source would be NUREG/CR-1278, Table 20-20, line 4, but negative dependence with a is assumed because b is the second half of a step that incorporates an OR; that is, a requires performance of one or the other of two operations.
c,C: Estimate. NUREG/CR-1278, Table 20-20, line 4.
d,D: Estimate. Normally there would be complete dependency between d and c; but this step is embedded in a procedure which requires most operations to take place on either of two panels, and d is the performance of an operation on the other panel (the operation must be performed on both). The negative dependency between actions d and c is due to a poorly-written procedure. Normally d would have a higher probability of success than c, up to complete dependency.
e,E: Estimate. NUREG/CR-1278, Table 20-20, line 4.
f,F: Estimate. NUREG/CR-1278, Table 20-20, line 4.
g,G: Estimate. See d (g relates to f as d relates to c).

REFERENCES:

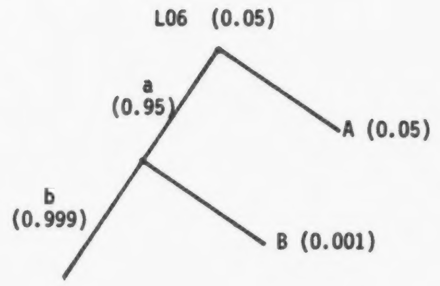
CR-3 Emergency Procedure EP-106, Loss of Reactor Coolant or Reactor Coolant Pressure, Rev. 22, 10/25/79.

Figure 5.6 Probability Estimation for Operator Fault H*02.

FAULT: Premature cutoff of low pressure coolant injection by operator, given a LOCA

BOOLEAN SYMBOL: L06

ESTIMATED PROBABILITY: 0.05



REQUIRED ACTIONS:

a: All operators leave LPI running when needed, even though it would properly have been turned off several times earlier in the sequence.
b: All operators recognize low pressure condition and leave LPI running.

ASSUMPTIONS:

1. Multiple operators work independently. Any one of them could commit a fault.

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: Estimate. Based on the "mind-sets" of operators under pressure. The LPI is repeatedly turned off and there are operators present who did not turn it off previously and thus may believe it should be turned off at this time.
b,B: The fault is that the operator responsible for monitoring primary system pressure will misread the pressure indicator, think the pressure is too high, and turn off LPI. NUREG/CR-1278, Table 20-5, line 1. The lower bound of uncertainty is used because this is a simple task being performed under high stress, which enhances performance of simple tasks.

REFERENCE:

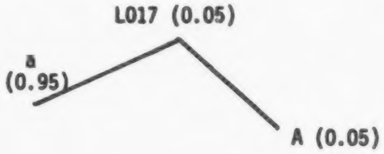
CR-3 Emergency Procedure EP-106, Loss of Reactor Coolant or Reactor Coolant Pressure, Pev. 22, 10/25/79.

Figure 5.7 Probability Estimation for Operator Fault L06.

FAULT: Premature initiation of recirculation, given a LOCA

BOOLEAN SYMBOL: L017

ESTIMATED PROBABILITY: 0.05



REQUIRED ACTION:

a: Operator bases decision on sump level indicator rather than on BWST low-level alarm.

ASSUMPTION:

1. Low-level setpoint will not fail or cause BWST alarm to go off too soon.

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: Estimate. NUREG/CR-1278, Table 20-20, line 5; the highest value is used since the operators report a false belief with respect to the cue for initiating recirculation.

REFERENCES:

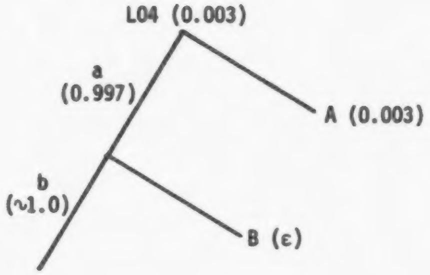
CR-3 Emergency Procedure EP-106, Loss of Reactor Coolant or Reactor Coolant Pressure, Rev. 22, 10/25/79.
Discussions with CR-3 operating personnel, November 1979.

Figure 5.8 Probability Estimation for Operator Fault L017.

FAULT: Delayed initiation of recirculation, given any LOCA

BOOLEAN SYMBOL: L04

ESTIMATED PROBABILITY: 0.003



REQUIRED ACTIONS:

a: Operator detects BWST low-level alarm
b: Operator begins recirculation

ASSUMPTIONS:

1. Probability based on one operator
2. Annunciator is one of about five actuated at the same time
3. Action is completely dependent upon alarm, since operating procedure has operator essentially waiting for the signal.

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: NUREG/CR-1278, Table 20-4, line 5
b,B: Estimate. Based on an assumption of complete dependency.

REFERENCES:

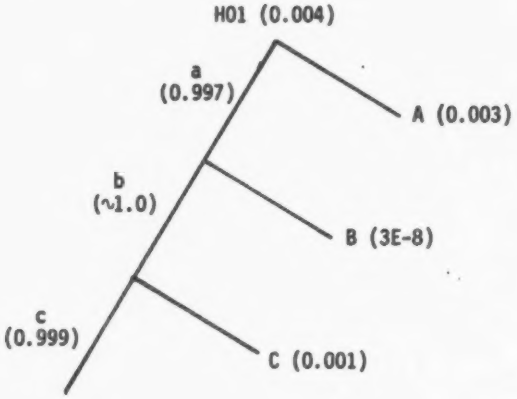
CR-3 Emergency Procedure EP-106, Loss of Reactor Coolant or Reactor Coolant Pressure, Rev. 22, 10/25/79.

Figure 5.9 Probability Estimation for Operator Fault L04.

FAULT: Premature cutoff of high pressure coolant injection by operator, given B4, B3 or transient-induced LOCA

BOOLEAN SYMBOL: H01

ESTIMATED PROBABILITY: 0.004



REQUIRED ACTIONS:

a: Operator correctly reads LPI flow indicator
b: Operator correctly calculates subcooling
c: Operator adequately throttles HPI system

ASSUMPTIONS:

1. Analysis based on single operator
2. Correct subcooling curves will be read, as there is no similar page nearby in the plant operations book

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: NUREG/CR-1278, Table 20-12 line 4
b,B: NUREG/CR-1278, Table 20-12 line 4, six meters. Adjusted for dependent readings with a tendency for recovery (noting an error on reading four meters will tend to produce correction of errors on meters 1-3, etc.) by treating as three independent readings.
c,C: Estimate. Action is considered a complex task performed under stress (relatively high error probability), but one in which a gross error is required to cause any trouble.

REFERENCES:

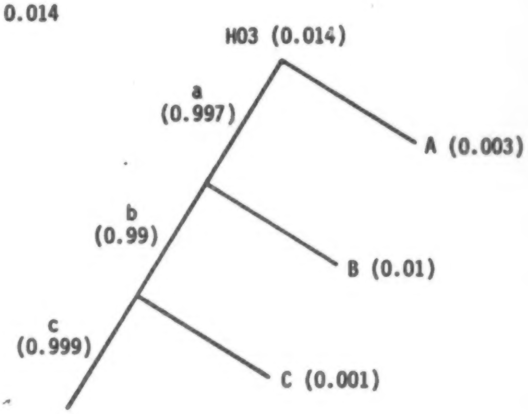
CR-3 Emergency Procedure EP-106, Loss of Reactor Coolant or Reactor Coolant Pressure, Rev. 22, 10/25/79.
CR-3 Operating Procedure OP-103, Plant Curve Book, Rev. 20, 9/20/79.

Figure 5.10 Probability Estimation for Operator Fault H01.

FAULT: Failure to establish a feed and bleed operation, given a transient with loss of all secondary cooling.

BOOLEAN SYMBOL: H03

ESTIMATED PROBABILITY: 0.014



REQUIRED ACTIONS:

a: Operator detects alarm indicating pressure or temperature deviation
b: Operator takes action to initiate feed-and-bleed
c: Operator chooses correct controls for feed-and-bleed operation

ASSUMPTIONS:

1. Analysis based on single operator
2. Pressure and temperature alarms are two out of about five that will sound at one time
3. Control relationship to other controls assumed to be typical
4. Moderate (optimal) stress assumed -- 15 minutes to perform task

SOURCES OR BASES OF PROBABILITY ESTIMATES:

a,A: NUREG/CR-1278, Table 20-4, line 5
b,B: This requires diagnosis of problem and choice of correct procedure, which must be done within a time window of about 20 minutes. The probability is based on the assumption that the operator is not likely to misdiagnose the condition. ATWS is the only condition with similar symptoms, and the reactor will not trip on ATWS, so it is noticeably different. Note, however, that this event includes the possibility of the operator regarding the symptoms as unimportant, as well as his regarding them as symptoms of a different problem.
c,C: Estimate. NUREG/CR-1278, Table 20-19, typical value

REFERENCES:

CR-3 Emergency Procedure EP-108, Loss of Steam Generator Feed, Rev. 10, 8/2/79.
CR-3 Emergency Procedure EP-103, Loss of RC Flow/RC Pump Trip, Rev. 8, 8/2/79.

Figure 5.11 Probability Estimation for Operator Fault H03.

References

5-1 U.S. Nuclear Regulatory Commission, "Reactor Safety Study-An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants," WASH-1400 (NUREG-75/014), October 1975.

5-2 R. C. Erdmann, F. L. Leverenz, H. Kirch and G. S. Lellouche, Electric Power Research Institute, "WAMCUT, A Computer Code for Fault Tree Evaluation," EPRI NP-803, 1978.

5-3 Letter from Joseph Murphy, NRC, to David Carlson, Sandia National Laboratories, Subject: Component Failure Rates to be used for IREP Quantification, September 26, 1980.

5-4 Edison Electric Institute, "Report on Equipment Availability for the Ten Year Period 1967-1976," Publication No. 77-64, 1977.

5-5 W. H. Sullivan and J. P. Poloski, EG&G Idaho, Inc., "Data Summaries of Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants, January 1, 1972 to April 30, 1978," USNRC Report NUREG/CR-1205, January 1980.

5-6 Edward J. Friedman, George E. Mouchahoir, Oscar G. Farah, Robert P. Ouellette and P. N. Cheremisinoff, Electrotechnology, Volume 3, Chapter 8, Ann Arbor Science Publishers, Inc.

5-7 Hans Bode, Lead Acid Batteries, (John Wiley & Sons, 1977, translation), Section 4.5.

5-8 Letter from Ronald M. Bright, Florida Power Corporation, to Frank Rowsome, NRC, Subject: Utility Review of SAI report "Brief Results to Date Crystal River-3 Safety Study", April 29, 1980.

5-9 Letter from Abel A. Garcia, SAI, to Patsy Baynard, Florida Power Corporation, Subject: Florida Power Comments on the Crystal River-3 Safety Study, September 18, 1980.

5-10 A. D. Swain and H. E. Guttmann, Sandia Laboratories, "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, " USNRC Report NUREG/CR-1278, April 1980.

5-11 D. M. Rasmuson, G. R. Burdick, and J. R. Wilson, EG&G Idaho, Inc., "Common Cause Failure Analysis Techniques: A Review and Comparative Evaluation," Report No. TREE-1349, September 1979.

5-12 J. A. Stevenson and C. L. Atwood, Idaho National Engineering Laboratory, "Common Cause and Individual Failure and Fault Rates for Licensee Event Reports of Diesel Generators at U.S. Commercial Nuclear Power Plants-Draft", Report No EGG-EA-5359, February 1981.

5-13 C. J. Atwood, Idaho National Engineering Laboratory, "Common Cause and Individual Failure and Fault Rates for Licensee Event Reports of Pumps at U.S. Commercial Nuclear Power Plants-Draft," Report No. EGG-EA-5289, November 1980.

5-14 Technical Specifications; Appendix A to the Operating License for Crystal River-Unit 3.

5-15 F. L. Leverenz, Jr., J. M. Koren, R. C. Erdmann and G. S. Lellouche, Electric Power Research Institute, "ATWS: A Reappraisal Part III Frequency of Anticipated Transients," EPRI NP-801, July 1978.

5-16 D. W. LaBelle, J. E. Koske and J. F. Scott,Babcock and Wilcox, "Babcock and Wilcox Anticipated Transients Without Scram Analysis," Report No BAW-10099, December 1974.

5-17 A. F. McBride, D. W. LaBelle, J. R. Lovell, E. Oelkers, and C. S. Banwarth, Babcock and Wilcox, "Babcock and Wilcox Anticipated Transients Without Scram Analysis, "Report No BAW-10099, Rev. 1, May 1977.

5-18 C. J. Kolb, S. W. Hatch, P. Cybulskis and R. O. Wooton, Sandia National Laboratories, "Reactor Safety Study Methodology Applications Program: Oconee No 3 PWR Power Plant," USNRC Report NUREG/CR-1659 (2 of 4) January 1981, Revised May 1981.

5-19 The President's Commission on the Accident at Three Mile Island, "The Accident at Three Mile Island, October 1979.

Distribution:

USNRC Distribution Contractor (CDSI) (155)
7300 Pearl Street
Bethesda, Maryland 20014
130 Copies for AN
25 Copies for NTIS

Author selected distribution - 25 Copies
(List available from author.)

4400	A. W. Snyder
4410	D. J. McCloskey
4412	J. W. Hickman (3)
4412	D. D. Carlson
4412	W. R. Cramond
4412	D. D. Drayer
4412	F. T. Harper
4412	S. W. Hatch
4412	A. M. Kolaczkowski
4412	G. J. Kolb
4412	A. C. Payne
4412	R. G. Spulak
4412	T. A. Wheeler
4413	N. R. Ortiz
4414	G. B. Varnado
4415	D. J. McCloskey, Actg.
4416	L. D. Chapman
3141	L. J. Erickson (5)
3151	W. L. Garner (3)
8214	M. A. Pound